

## User Manual

## Configuration

## MTS Series Switch

The naming of copyright trademarks in this manual shall not be considered as meaning that such names are regarded free of charge in the sense of the Trademark and Trade Name Protection Law, and therefore they shall not be considered freely usable to anyone, even if not otherwise specified.

## **Proprietary Notices**

© 2021 Belden Singapore Pte Ltd.

This manual and corresponding software are subject to copyright protection. All rights reserved. They shall not be reproduced, copied, translated, or converted in whole or in part into any electronic media or machine scannable format. One exception is to make backup software for your own use. The end user license agreement on the accompanying CD/DVD applies for devices with embedded software.

The performance features described herein are binding only after they are clearly agreed upon when the contract is signed. This document is produced by Belden Singapore Pte Ltd. based on the company's knowledge as far as possible. Belden Singapore Pte Ltd. reserves the right to change the content of this document without prior notice. Belden Singapore Pte Ltd. offers no guarantee on the correctness or accuracy of the information in this document.

Belden Singapore Pte Ltd. assumes no responsibility for damages caused by the use of network components or related operating software. In addition, we also invoke the conditions of use stipulated in the license contract.

## **Safety Notice**

**IMPORTANT!** Before powering on the product, please read the safety and compatibility information of the product.

## **Environmental Statement**

This product meets the design requirements for environmental protection. The storage, use and disposal of the product shall comply with relevant national laws and regulations.

## **Target Readers**

This manual mainly applies to the following persons:

- Commissioning Engineer
- Field Maintenance Engineer
- System Maintenance Engineer

## **Manual Conventions**

Screen Output Format Conventions

FORMAT	Description
Screen print	indicates screen output information.
<b>Keywords of Screen print</b>	The red information represents the key information in the screen output.

### Icon and Symbol Conventions

FORMAT	Description
 <b>Note:</b>	Supplements or emphasizes the foregoing information.
 <b>Notice:</b>	Indicates the content that needs to be paid attention to during the installation or use of the device, which is the key to the correct installation and operation of the device.
 <b>Warning:</b>	Operations prohibited or operations that must be performed in accordance with prescribed steps, otherwise they may cause personal injury or device damage.

### Command Format Conventions

FORMAT	Description
<b>bold</b>	Command line keywords (the part of a command that remains unchanged and must be input so) are represented in <b>Bold Font</b> .
<i>italic</i>	Command line parameters (the part of a command that must be replaced by actual values) are represented in <i>Italic</i> .
Curly bracket "{ }"	Indicates that the option in the brackets is mandatory.
Square brackets "[ ]"	Indicates that the option in the brackets is optional.
Angle brackets "<>"	Indicates that the information in the brackets will not be displayed.
Boldface square brackets "【 】"	Indicates that the content in the brackets requires the user's attention.
Pipe " "	used for separating several options, and indicates selecting one of two or one of many.

FORMAT	Description
Slash "/"	For separating several options, it indicates that the separated options are applicable at the same time.
Sign "#"	Lines starting with a "#" are represented as comment lines.

The icons used in this manual and their meanings are as follows:

Icon	Description
	This icon and its related description represent the switch in a general sense.
	This icon and its related description represent a router in a general sense.

## Access to Our Information

The latest version of this manual is available from the Hirschmann product website at:

[www.doc.hirschmann.com](http://www.doc.hirschmann.com).

## Technical Support

Belden Singapore Pte Ltd.

51 Lorong Chuan #05-01

New Tech Park

Singapore 556741

Tel: +65 68799800

## Revision History

The revision history includes the description for each manual update. The latest version of the manual contains the updated contents of all previous manual versions.

REVISION DATE	Revision Details
November 30, 2020	Released for the first time

# Contents

<b>1</b>	<b>SYSTEM OPERATION BASICS</b>	<b>54</b>
<b>1.1</b>	<b>OVERVIEW</b>	<b>54</b>
<b>1.2</b>	<b>SYSTEM OPERATION BASIC FUNCTIONS</b>	<b>54</b>
1.2.1	DEVICE CONFIGURATION MODE	54
1.2.2	COMMAND OPERATING MODE	55
1.2.3	COMMAND LINE INTERFACE	57
<b>2</b>	<b>SYSTEM LOGIN</b>	<b>63</b>
<b>2.1</b>	<b>OVERVIEW</b>	<b>63</b>
<b>2.2</b>	<b>SYSTEM LOGIN FUNCTION CONFIGURATION</b>	<b>63</b>
2.2.1	LOGGING IN TO THE DEVICE THROUGH THE CONSOLE PORT	64
2.2.2	CONFIGURING REMOTE LOGIN THROUGH TELNET	66
2.2.3	CONFIGURING REMOTE LOGIN THROUGH SSH	68
<b>2.2.4</b>	<b>CONFIGURE REMOTE LOGIN THROUGH WEB</b>	<b>69</b>
2.2.5	SYSTEM LOGIN MONITORING AND MAINTAINING	71
<b>2.3</b>	<b>TYPICAL CONFIGURATION OF SYSTEM LOGIN EXAMPLE</b>	<b>72</b>
2.3.1	CONFIGURE A LOCAL TERMINAL TO TELNET TO THE DEVICE	72
2.3.2	CONFIGURE A LOCAL DEVICE TO LOG IN TO A REMOTE DEVICE VIA TELNET	73
2.3.3	CONFIGURE A LOCAL DEVICE TO LOG IN TO A REMOTE DEVICE VIA SSH	74
2.3.4	CONFIGURE A DEVICE AS AN SFTP CLIENT	76
2.3.5	CONFIGURE A DEVICE AS AN SFTP SERVER	77
2.3.6	CONFIGURE A LOCAL DEVICE TO LOG IN TO A REMOTE DEVICE VIA SSH PUBLIC KEY AUTHENTICATION	79
<b>3</b>	<b>SYSTEM CONTROL AND MANAGEMENT</b>	<b>84</b>
<b>3.1</b>	<b>OVERVIEW</b>	<b>84</b>
<b>3.2</b>	<b>LOGIN CONTROL AND MANAGEMENT FUNCTION CONFIGURATION</b>	<b>84</b>
3.2.1	SWITCH OVER BETWEEN USER LEVELS	85
3.2.2	CONFIGURE THE COMMAND LEVEL	87
3.2.3	CONFIGURE THE ENABLE PASSWORD	87
3.2.4	CONFIGURE LINE PROPERTIES	88
3.2.5	SYSTEM CONTROL AND MANAGEMENT MONITORING AND MAINTAINING	94
<b>4</b>	<b>FTP, FTPS, TFTP AND SFTP</b>	<b>95</b>
<b>4.1</b>	<b>OVERVIEW</b>	<b>95</b>

<b>4.2</b>	<b>FTP, FTPS, TFTP AND SFTP FUNCTION CONFIGURATION.....</b>	<b>96</b>
4.2.1	CONFIGURE AN FTP SERVER. ....	96
4.2.2	CONFIGURE AN FTP CLIENT. ....	98
4.2.3	CONFIGURE A TFTP CLIENT. ....	99
4.2.4	CONFIGURE THE TFTP SERVER.....	100
4.2.5	CONFIGURE AN SFTP SERVER.....	100
4.2.6	CONFIGURE AN SFTP CLIENT.....	101
4.2.7	FTP AND TFTP MONITORING AND MAINTAINING.....	101
<b>4.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF FTP AND TFTP .....</b>	<b>101</b>
4.3.1	CONFIGURE A DEVICE AS AN FTP CLIENT.....	101
4.3.2	CONFIGURE A DEVICE AS AN FTP SERVER.....	103
4.3.3	CONFIGURE A DEVICE AS AN TFTP CLIENT.....	106
4.3.4	CONFIGURE A DEVICE AS AN SFTP CLIENT.....	108
4.3.5	CONFIGURE A DEVICE AS AN SFTP SERVER.....	109
4.3.6	CONFIGURE A DEVICE AS AN FTPS CLIENT.....	110
<b>5</b>	<b>FILE SYSTEM MANAGEMENT .....</b>	<b>115</b>
<b>5.1</b>	<b>OVERVIEW.....</b>	<b>115</b>
<b>5.2</b>	<b>FILE SYSTEM MANAGEMENT FUNCTION CONFIGURATION.....</b>	<b>115</b>
5.2.1	MANAGE STORAGE DEVICES. ....	116
5.2.2	MANAGE FILE DIRECTORIES.....	117
5.2.3	MANAGE FILE OPERATIONS.....	119
5.2.4	DOWNLOAD A FILE FROM FTP.....	121
5.2.5	CONFIGURE STARTUP PARAMETERS.....	122
5.2.6	FILE SYSTEM MANAGING, MONITORING, AND MAINTAINING.....	123
<b>5.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF FILE SYSTEM MANAGEMENT.....</b>	<b>123</b>
5.3.1	CONFIGURE STARTUP PARAMETERS.....	123
<b>6</b>	<b>CONFIGURATION FILE MANAGEMENT.....</b>	<b>125</b>
<b>6.1</b>	<b>OVERVIEW.....</b>	<b>125</b>
<b>6.2</b>	<b>CONFIGURATION FILE MANAGEMENT FUNCTION CONFIGURATION.....</b>	<b>126</b>
6.2.1	SAVE THE CURRENT CONFIGURATION.....	126
6.2.2	CONFIGURE THE BACKUP SYSTEM.....	127
6.2.3	RESTORE THE STARTUP CONFIGURATION.....	128
6.2.4	CONFIGURATION FILE MANAGING, MONITORING, AND MAINTAINING.....	129

6.2.5	CONFIGURATION FILE ENCRYPTION.....	130
<b>7</b>	<b>SYSTEM MANAGEMENT.....</b>	<b>131</b>
<b>7.1</b>	<b>OVERVIEW.....</b>	<b>131</b>
<b>7.2</b>	<b>SYSTEM MANAGEMENT FUNCTION CONFIGURATION.....</b>	<b>131</b>
7.2.1	CONFIGURE THE DEVICE NAME.....	132
7.2.2	CONFIGURE THE SYSTEM TIME AND TIME ZONE.....	132
7.2.3	CONFIGURE THE LOGIN WELCOME MESSAGE.....	133
7.2.4	CONFIGURE THE SYSTEM EXCEPTION PROCESSING MODE.....	133
7.2.5	CONFIGURE TO RESTART THE DEVICE.....	135
7.2.6	CONFIGURE THE HISTORY COMMAND SAVING FUNCTION.....	136
7.2.7	CONFIGURE THE LOGIN SECURITY SERVICE.....	136
7.2.8	CONFIGURE CPU MONITORING.....	138
7.2.9	CONFIGURE DISPLAY OF PROPERTIES IN PAGES.....	138
7.2.10	OPERATION RECORD FILE MANAGEMENT.....	139
7.2.11	CONFIGURE SYSTEM SECURITY MODE.....	139
7.2.12	SYSTEM MANAGING, MONITORING, AND MAINTAINING.....	140
7.2.13	CONFIGURE THE FLEXIBLE TABLE ENTRY MODE.....	141
<b>7.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF SYSTEM MANAGEMENT.....</b>	<b>142</b>
7.3.1	CONFIGURE USER- AND IP-BASED LOGIN RESTRICTIONS.....	142
7.3.2	CONFIGURE QUICK LOGIN RESTRICTIONS.....	144
<b>8</b>	<b>SYSTEM ALARM.....</b>	<b>146</b>
<b>8.1</b>	<b>OVERVIEW.....</b>	<b>146</b>
<b>8.2</b>	<b>SYSTEM ALARM FUNCTION CONFIGURATION.....</b>	<b>146</b>
8.2.1	CONFIGURE SYSTEM TEMPERATURE ALARMS.....	146
8.2.2	CONFIGURE SYSTEM CPU ALARMS.....	147
8.2.3	CONFIGURE THE LOW THRESHOLD OF MEMORY USAGE.....	148
8.2.4	CONFIGURE SYSTEM MEMORY ALARMS.....	148
8.2.5	CONFIGURE SYSTEM POWER SUPPLY ALARMS.....	149
8.2.6	CONFIGURE SYSTEM FAN ALARMS.....	149
<b>9</b>	<b>SYSTEM LOG CONFIGURATION.....</b>	<b>150</b>
<b>9.1</b>	<b>OVERVIEW.....</b>	<b>150</b>
<b>9.2</b>	<b>SYSTEM LOG FUNCTION CONFIGURATION.....</b>	<b>151</b>
9.2.1	CONFIGURE LOG OUTPUT FUNCTIONS.....	152

9.2.2	CONFIGURE THE TIMESTAMP FOR LOGS.....	157
9.2.3	CONFIGURE OPERATION LOG OUTPUT TO THE LOG HOST .....	158
9.2.4	CONFIGURE LOG SUPPRESSION.....	159
9.2.5	CONFIGURE LOG FILES CAPACITY.....	159
9.2.6	CONFIGURE LOG FILES ENCRYPTION .....	160
9.2.7	CONFIGURE LOG DISPLAY COLOR.....	160
9.2.8	CONFIGURE LOG FILTERING FUNCTION .....	162
9.2.9	CONFIGURE THE ORIGIN-ID OF A DEVICE.....	162
9.2.10	LOG MONITORING AND MAINTAINING.....	163
<b>10</b>	<b>SOFTWARE UPGRADE .....</b>	<b>164</b>
<b>10.1</b>	<b>OVERVIEW.....</b>	<b>164</b>
<b>10.2</b>	<b>SOFTWARE UPGRADE FUNCTION CONFIGURATION .....</b>	<b>166</b>
10.2.1	UPGRADE THE IMAGE PROGRAM PACKAGE .....	167
10.2.2	PATCH PROGRAM UPGRADE.....	169
10.2.3	CMM PROGRAM UPGRADE.....	170
10.2.4	BOOTLOADER PROGRAM UPGRADE .....	172
10.2.5	DEVINFO FILE UPGRADE.....	176
10.2.6	PACKAGE FILE UPGRADE.....	177
<b>10.3</b>	<b>EXAMPLE OF TYPICAL CONFIGURATION FOR SOFTWARE UPGRADE.....</b>	<b>180</b>
10.3.1	UPGRADE PACKAGE FILE .....	180
10.3.2	FULL UPGRADE OF ALL SOFTWARE VERSIONS .....	183
10.3.3	UPGRADE BOOTLOADER USING CONSOLE PORT.....	188
<b>11</b>	<b>BOOTLOADER .....</b>	<b>190</b>
<b>11.1</b>	<b>OVERVIEW.....</b>	<b>190</b>
<b>11.2</b>	<b>BOOTLOADER FUNCTION CONFIGURATION .....</b>	<b>190</b>
11.2.1	PREPARATION FOR BOOTLOADER FUNCTION CONFIGURATION .....	191
11.2.2	ENTER THE BOOTLOADER CONFIGURATION MODE .....	191
11.2.3	SET BOOTLOADER STARTUP PARAMETERS.....	192
11.2.4	UPGRADE BOOTLOADER PROGRAM.....	193
11.2.5	BOOTLOADER MONITORING AND MAINTAINING .....	195
<b>11.3</b>	<b>BOOTLOADER TYPICAL CONFIGURATION EXAMPLE .....</b>	<b>195</b>
11.3.1	CONFIGURE THE BOOTLOADER TO START THE IMAGE PROGRAM VIA THE NETWORK. ....	195
<b>12</b>	<b>POE MANAGEMENT .....</b>	<b>196</b>

<b>12.1</b>	<b>OVERVIEW.....</b>	<b>197</b>
<b>12.1.1</b>	<b>PD (POWER DEVICE): DEVICES THAT RECEIVE POWER. THE POWER OF THE DEVICES IS USUALLY NOT LARGE. PSE/PD INTERFACE SPECIFICATIONS.....</b>	<b>197</b>
<b>12.1.2</b>	<b>POE POWER SUPPLY PROCESS.....</b>	<b>198</b>
<b>12.2</b>	<b>POE FUNCTION CONFIGURATION.....</b>	<b>199</b>
<b>12.2.1</b>	<b>POE BASIC FUNCTION CONFIGURATION.....</b>	<b>201</b>
<b>12.2.2</b>	<b>CONFIGURE THE POE POWER.....</b>	<b>204</b>
<b>12.2.3</b>	<b>CONFIGURE POWER SUPPLY PRIORITIES.....</b>	<b>206</b>
<b>12.2.4</b>	<b>CONFIGURE PD POWER-UP AND POWER-DOWN PARAMETERS.....</b>	<b>208</b>
<b>12.2.5</b>	<b>CONFIGURE THE ABNORMALITY RECOVERY FUNCTION.....</b>	<b>211</b>
<b>12.2.6</b>	<b>CONFIGURE POE POWER ALARM THRESHOLD.....</b>	<b>213</b>
<b>12.2.7</b>	<b>POE MONITORING AND MAINTAINING.....</b>	<b>213</b>
<b>13</b>	<b>PDI.....</b>	<b>214</b>
<b>13.1</b>	<b>OVERVIEW.....</b>	<b>214</b>
<b>13.2</b>	<b>CONFIGURE PDI BASIC FUNCTIONS.....</b>	<b>214</b>
<b>13.3</b>	<b>CONFIGURE THE ARP PACKET DELIVERY INTERVAL.....</b>	<b>215</b>
<b>13.4</b>	<b>CONFIGURE THE NUMBER OF RETRIES FOR ARP PACKET DELIVERY.....</b>	<b>215</b>
<b>13.5</b>	<b>CONFIGURING IP INSPECTION TABLE ENTRIES.....</b>	<b>216</b>
<b>13.6</b>	<b>PDI MONITORING AND MAINTAINING.....</b>	<b>216</b>
<b>14</b>	<b>LUM.....</b>	<b>217</b>
<b>14.1</b>	<b>OVERVIEW.....</b>	<b>217</b>
<b>14.2</b>	<b>LUM FUNCTION CONFIGURATION.....</b>	<b>217</b>
<b>14.2.1</b>	<b>CONFIGURE ACCESS.....</b>	<b>218</b>
<b>14.2.2</b>	<b>CONFIGURE LOCAL USERS.....</b>	<b>220</b>
<b>14.2.3</b>	<b>CONFIGURE ADMINISTRATOR USER ATTRIBUTES.....</b>	<b>221</b>
<b>14.2.4</b>	<b>CONFIGURE ACCESS USER ATTRIBUTES.....</b>	<b>224</b>
<b>14.2.5</b>	<b>CONFIGURE LOCAL USER GROUPS.....</b>	<b>225</b>
<b>14.2.6</b>	<b>CONFIGURE PASSWORD POLICIES.....</b>	<b>227</b>
<b>14.2.7</b>	<b>LUM MONITORING AND MAINTAINING.....</b>	<b>230</b>
<b>14.3</b>	<b>TYPICAL LUM CONFIGURATION EXAMPLE.....</b>	<b>231</b>
<b>14.3.1</b>	<b>CONFIGURE NETWORK ADMINISTRATOR USERS.....</b>	<b>231</b>
<b>15</b>	<b>ZTP.....</b>	<b>232</b>
<b>15.1</b>	<b>OVERVIEW.....</b>	<b>232</b>

<b>15.2 ZTP FUNCTION CONFIGURATION</b> .....	<b>234</b>
15.2.1 ENABLE OR DISABLE ZTP FUNCTION .....	234
15.2.2 ZTP MONITORING AND MAINTAINING.....	235
<b>15.3 ZTP TYPICAL CONFIGURATION EXAMPLE</b> .....	<b>235</b>
15.3.1 CONFIGURE ZTP TO USE COMMON INTERMEDIATE FILES FOR ZERO-CONFIGURATION DEPLOYMENT VIA DHCP .....	235
15.3.2 CONFIGURE ZTP TO USE PYTHON INTERMEDIATE FILES FOR ZERO-CONFIGURATION DEPLOYMENT VIA DHCP .....	239
15.3.3 CONFIGURE ZTP TO USE COMMON INTERMEDIATE FILES FOR ZERO-CONFIGURATION DEPLOYMENT VIA USB.....	242
15.3.4 CONFIGURE ZTP TO USE PYTHON INTERMEDIATE FILES FOR ZERO-CONFIGURATION DEPLOYMENT VIA USB.....	245
15.3.5 CONFIGURE ZTP TO AUTOMATICALLY COMPLETE STACKING USING PYTHON INTERMEDIATE FILES VIA DHCP .....	248
<b>16 INTERFACE BASIS</b> .....	<b>255</b>
<b>16.1 OVERVIEW</b> .....	<b>255</b>
<b>16.2 BASIC FUNCTION CONFIGURATION OF INTERFACES</b> .....	<b>256</b>
16.2.1 CONFIGURE THE BASIC FUNCTIONS OF THE INTERFACES .....	256
16.2.2 CONFIGURE THE INTERFACE GROUP FUNCTION .....	260
16.2.3 CONFIGURE INTERFACE STATUS SNMP AGENT CARE LEVEL.....	261
16.2.4 BASIC MONITORING AND MAINTAINING OF INTERFACES .....	262
<b>17 ETHERNET INTERFACE</b> .....	<b>263</b>
<b>17.1 OVERVIEW</b> .....	<b>263</b>
<b>17.2 ETHERNET INTERFACE FUNCTION CONFIGURATION</b> .....	<b>264</b>
17.2.1 CONFIGURE BASIC FUNCTIONS OF PORT.....	265
17.2.2 CONFIGURE PORT DETECTION FUNCTION.....	283
17.2.3 CONFIGURE STORM SUPPRESSION .....	284
17.2.4 CONFIGURE PORT UNI/NNI TYPE.....	286
17.2.5 CONFIGURE BASIC FUNCTIONS OF L3 ETHERNET INTERFACE .....	288
17.2.6 ETHERNET INTERFACE MONITORING AND MAINTAINING .....	290
<b>17.3 TYPICAL CONFIGURATION EXAMPLE OF ETHERNET INTERFACE</b> .....	<b>291</b>
17.3.1 CONFIGURE STORM SUPPRESSION FUNCTION.....	291
<b>18 AGGREGATION GROUP INTERFACE</b> .....	<b>294</b>
<b>18.1 OVERVIEW</b> .....	<b>294</b>
<b>18.2 AGGREGATION GROUP INTERFACE FUNCTION CONFIGURATION</b> .....	<b>294</b>

18.2.1	CONFIGURE BASIC FUNCTIONS OF L3 AGGREGATION GROUP INTERFACE .....	294
18.2.2	MONITORING AND MAINTAINING OF AGGREGATION GROUP INTERFACE .....	296
<b>19</b>	<b>VLAN INTERFACE .....</b>	<b>297</b>
<b>19.1</b>	<b>OVERVIEW.....</b>	<b>297</b>
<b>19.2</b>	<b>VLAN INTERFACE FUNCTION CONFIGURATION .....</b>	<b>297</b>
19.2.1	CONFIGURE THE BASIC FUNCTIONS OF THE VLAN INTERFACE .....	297
19.2.2	VLAN INTERFACE MONITORING AND MAINTAINING .....	300
<b>19.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF VLAN INTERFACE .....</b>	<b>301</b>
19.3.1	CONFIGURE VLAN INTERFACE .....	301
<b>20</b>	<b>LOOPBACK INTERFACE.....</b>	<b>303</b>
<b>20.1</b>	<b>OVERVIEW.....</b>	<b>303</b>
<b>20.2</b>	<b>LOOPBACK INTERFACE FUNCTION CONFIGURATION .....</b>	<b>303</b>
20.2.1	CONFIGURE THE BASIC FUNCTIONS OF THE LOOPBACK INTERFACE .....	303
<b>21</b>	<b>NULL INTERFACE .....</b>	<b>306</b>
<b>21.1</b>	<b>OVERVIEW.....</b>	<b>306</b>
<b>21.2</b>	<b>NULL INTERFACE FUNCTION CONFIGURATION .....</b>	<b>306</b>
21.2.1	CONFIGURE THE BASIC FUNCTIONS OF THE NULL INTERFACE .....	306
<b>22</b>	<b>VIRTUAL SWITCH LINK INTERFACE .....</b>	<b>308</b>
<b>22.1</b>	<b>OVERVIEW.....</b>	<b>308</b>
<b>22.2</b>	<b>VIRTUAL SWITCH LINK INTERFACE FUNCTION CONFIGURATION.....</b>	<b>308</b>
22.2.1	CONFIGURE FUNCTIONS OF THE VIRTUAL SWITCH LINK INTERFACE .....	308
22.2.2	MONITORING AND MAINTAINING OF VIRTUAL SWITCH LINK INTERFACE .....	309
<b>23</b>	<b>TUNNEL INTERFACE .....</b>	<b>310</b>
<b>23.1</b>	<b>OVERVIEW.....</b>	<b>310</b>
<b>23.2</b>	<b>TUNNEL INTERFACE FUNCTION CONFIGURATION.....</b>	<b>310</b>
23.2.1	CONFIGURE THE BASIC FUNCTIONS OF THE TUNNEL INTERFACE .....	310
23.2.2	TUNNEL INTERFACE MONITORING AND MAINTAINING .....	311
<b>24</b>	<b>VXLAN INTERFACE .....</b>	<b>312</b>
<b>24.1</b>	<b>OVERVIEW.....</b>	<b>312</b>
<b>24.2</b>	<b>VXLAN INTERFACE FUNCTION.....</b>	<b>312</b>
24.2.1	CONFIGURE BASIC FUNCTIONS OF THE VXLAN INTERFACE .....	313
24.2.2	CONFIGURE DISTRIBUTED GATEWAY FUNCTION OF VXLAN.....	313
24.2.3	VXLAN INTERFACE MONITORING AND MAINTAINING .....	314

<b>25</b>	<b>LINK AGGREGATION</b>	<b>314</b>
<b>25.1</b>	<b>OVERVIEW</b>	<b>314</b>
25.1.1	BASIC CONCEPTS	315
25.1.2	LINK AGGREGATION MODES	316
<b>25.2</b>	<b>OVERVIEW</b>	<b>318</b>
25.2.1	LOAD BALANCING	318
25.2.2	HASH KEY	318
25.2.3	LOAD BALANCING MODE	320
<b>25.3</b>	<b>FUNCTION CONFIGURATION OF LOAD BALANCING MODE</b>	<b>320</b>
25.3.1	ENTER THE LOAD BALANCING MODE	321
25.3.2	CONFIGURE THE HASH KEY OF LOAD BALANCING MODE	322
25.3.3	CONFIGURE THE DEEP ANALYSIS ALGORITHM FOR IPV4/IPV6 PACKET OF LOAD BALANCING MODE	324
25.3.4	CONFIGURE THE DEEP ANALYSIS ALGORITHM FOR MPLS AND VXLAN PACKET OF LOAD BALANCING MODE	324
25.3.5	CONFIGURE THE LOAD SELECTION FOR IP TUNNEL PACKET OF LOAD BALANCING MODE	325
25.3.6	CONFIGURE THE LOAD SELECTION FOR MPLS, VXLAN AND TRILL PACKET OF LOAD BALANCING MODE	328
25.3.7	CONFIGURE HASH ALGORITHM SELECTION FOR LAC AND ECMP OF LOAD BALANCING MODE	329
25.3.8	CONFIGURE ALGORITHM SELECTION FOR IPV6 ADDRESS COMPRESSION OF LOAD BALANCING MODE	330
<b>25.4</b>	<b>LINK AGGREGATION FUNCTION CONFIGURATION</b>	<b>331</b>
25.4.1	CONFIGURE AN AGGREGATION GROUP	331
25.4.2	CONFIGURE LACP PRIORITIES	333
25.4.3	CONFIGURE HOT PLUG FOR RAPID SWITCH OF ROOT PORT	334
25.4.4	LINK AGGREGATION MONITORING AND MAINTAINING	335
<b>25.5</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF LINK AGGREGATION</b>	<b>336</b>
25.5.1	CONFIGURE A STATIC AGGREGATION GROUP	336
25.5.2	CONFIGURE A DYNAMIC AGGREGATION GROUP	339
<b>26</b>	<b>PORT ISOLATION</b>	<b>343</b>
<b>26.1</b>	<b>OVERVIEW</b>	<b>343</b>
<b>26.2</b>	<b>PORT ISOLATION FUNCTION CONFIGURATION</b>	<b>343</b>
26.2.1	CONFIGURE THE BASIC FUNCTION OF PORT ISOLATION	343
26.2.2	PORT ISOLATION MONITORING AND MAINTAINING	345

<b>26.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF PORT ISOLATION.....</b>	<b>345</b>
26.3.1	CONFIGURE PORT ISOLATION.....	345
<b>27</b>	<b>VLAN.....</b>	<b>348</b>
<b>27.1</b>	<b>OVERVIEW.....</b>	<b>348</b>
<b>27.2</b>	<b>VLAN FUNCTION CONFIGURATION.....</b>	<b>349</b>
27.2.1	CONFIGURE BASIC ATTRIBUTES FOR VLAN.....	350
27.2.2	CONFIGURE A PORT-BASED VLAN.....	351
27.2.3	CONFIGURE A MAC ADDRESS-BASED VLAN.....	356
27.2.4	CONFIGURE AN IP SUBNET-BASED VLAN.....	358
27.2.5	CONFIGURE AN IPV6 SUBNET-BASED VLAN.....	359
27.2.6	CONFIGURE A PROTOCOL-BASED VLAN.....	360
27.2.7	CONFIGURE THE TYPES OF FRAMES THAT CAN BE RECEIVED BY THE PORT.....	361
27.2.8	VLAN MONITORING AND MAINTAINING.....	362
<b>27.3</b>	<b>VLAN TYPICAL CONFIGURATION EXAMPLE.....</b>	<b>363</b>
27.3.1	CONFIGURE A PORT-BASED VLAN.....	363
27.3.2	CONFIGURE A MAC ADDRESS-BASED VLAN.....	365
27.3.3	CONFIGURE AN IP SUBNET-BASED VLAN.....	367
27.3.4	CONFIGURE AN IPV6 SUBNET-BASED VLAN.....	369
27.3.5	CONFIGURE A PROTOCOL-BASED VLAN.....	371
<b>28</b>	<b>QINQ AND VLAN MAPPING.....</b>	<b>373</b>
<b>28.1</b>	<b>OVERVIEW.....</b>	<b>373</b>
<b>28.2</b>	<b>QINQ AND VLAN MAPPING FUNCTION CONFIGURATION.....</b>	<b>373</b>
28.2.1	CONFIGURE BASIC QINQ FUNCTION.....	374
28.2.2	CONFIGURE PORT-BASED FLEXIBLE QINQ FUNCTION.....	375
28.2.3	CONFIGURE 1: 1 VLAN MAPPING FUNCTION.....	377
28.2.4	CONFIGURE N: 1 VLAN MAPPING FUNCTION.....	378
28.2.5	CONFIGURE THE PROTOCOL TYPE OF OUTER VLAN TAG OF THE PORT.....	380
28.2.6	CONFIGURE QINQ DROP FUNCTION.....	381
28.2.7	QINQ AND VLAN MAPPING MONITORING AND MAINTAINING.....	382
<b>28.3</b>	<b>EXAMPLE OF TYPICAL QINQ AND VLAN MAPPING CONFIGURATION.....</b>	<b>383</b>
28.3.1	CONFIGURE BASIC QINQ.....	383
28.3.2	CONFIGURE FLEXIBLE QINQ.....	385

28.3.3	CONFIGURE 1: 1 VLAN MAPPING .....	388
28.3.4	CONFIGURE N: 1 VLAN MAPPING.....	390
<b>29</b>	<b>SUPER-VLAN .....</b>	<b>393</b>
<b>29.1</b>	<b>OVERVIEW.....</b>	<b>393</b>
<b>29.2</b>	<b>VLAN FUNCTION CONFIGURATION .....</b>	<b>393</b>
29.2.1	CONFIGURE A SUPER VLAN.....	393
29.2.2	CONFIGURE SUB-VLAN MEMBERS OF THE SUPER-VLAN.....	394
29.2.3	ENABLE THE ARP PROXY FUNCTION.....	395
29.2.4	ENABLE THE ND PROXY FUNCTION.....	396
29.2.5	VLAN MONITORING AND MAINTAINING .....	397
<b>29.3</b>	<b>SUPER-VLAN TYPICAL CONFIGURATION EXAMPLE .....</b>	<b>397</b>
29.3.1	CONFIGURE A SUPER VLAN.....	397
<b>30</b>	<b>PVLAN .....</b>	<b>401</b>
<b>30.1</b>	<b>OVERVIEW.....</b>	<b>401</b>
<b>30.2</b>	<b>PVLAN FUNCTION CONFIGURATION.....</b>	<b>401</b>
30.2.1	CONFIGURE PRIMARY VLAN.....	402
30.2.2	ADD PORTS INTO PRIMARY VLAN .....	403
30.2.3	CONFIGURE SECONDARY VLAN.....	404
30.2.4	ADD PORTS INTO SECONDARY VLAN .....	404
30.2.5	CONFIGURE THE ASSOCIATION RELATIONSHIP BETWEEN PRIMARY VLAN AND SECONDARY VLAN	406
30.2.6	PVLAN MONITORING AND MAINTAINING.....	406
<b>30.3</b>	<b>TYPICAL PVLAN CONFIGURATION EXAMPLE .....</b>	<b>407</b>
30.3.1	CONFIGURE PVLAN .....	407
<b>31</b>	<b>VOICE-VLAN .....</b>	<b>410</b>
<b>31.1</b>	<b>OVERVIEW.....</b>	<b>410</b>
<b>31.2</b>	<b>VOICE-VLAN FUNCTION CONFIGURATION.....</b>	<b>410</b>
31.2.1	CONFIGURE A VOICE-VLAN .....	411
31.2.2	CONFIGURE AN OUI ADDRESS .....	411
31.2.3	ENABLE THE VOICE-VLAN FUNCTION OF A PORT.....	412
31.2.4	CONFIGURE THE VOICE-VLAN WORKING MODE ON THE PORT .....	413
31.2.5	ENABLE THE SECURITY MODE OF VOICE-VLAN.....	415
31.2.6	ENABLE THE LLDP-MED AUTHENTICATION MODE OF VOICE-VLAN.....	416

31.2.7	VOICE-VLAN MONITORING AND MAINTAINING .....	417
<b>31.3</b>	<b>VOICE-VLAN TYPICAL CONFIGURATION EXAMPLE .....</b>	<b>417</b>
31.3.1	CONFIGURE A VOICE-VLAN TO MANUAL MODE .....	417
31.3.2	CONFIGURE A VOICE-VLAN TO AUTOMATIC MODE .....	419
31.3.3	CONFIGURE THE SECURITY MODE OF VOICE-VLAN.....	421
31.3.4	CONFIGURE THE LLDP-MED AUTHENTICATION MODE OF VOICE-VLAN.....	423
<b>32</b>	<b>MAC ADDRESS TABLE MANAGEMENT .....</b>	<b>426</b>
<b>32.1</b>	<b>OVERVIEW.....</b>	<b>426</b>
<b>32.2</b>	<b>MAC ADDRESS MANAGEMENT FUNCTION CONFIGURATION .....</b>	<b>427</b>
32.2.1	CONFIGURE MANAGEMENT PROPERTIES OF MAC ADDRESSES. ....	428
32.2.2	CONFIGURE LIMITATIONS ON MAC ADDRESS LEARNING. ....	430
32.2.3	CONFIGURE STATIC MAC ADDRESSES.....	433
32.2.4	MAC ADDRESS MANAGEMENT MONITORING AND MAINTAINING.....	436
<b>32.3</b>	<b>FUNCTION CONFIGURATION FOR SOFTWARE LEARNING.....</b>	<b>437</b>
32.3.1	FUNCTION CONFIGURATION FOR SOFTWARE LEARNING .....	437
32.3.2	MONITORING AND MAINTENANCE OF SOFTWARE LEARNING FUNCTION .....	439
<b>32.4</b>	<b>CONFIGURE FUNCTION OF MAC ADDRESS MIGRATION LOG .....</b>	<b>439</b>
32.4.1	CONFIGURE FUNCTION OF MAC ADDRESS MIGRATION LOG .....	439
32.4.2	MONITORING AND MAINTENANCE OF MAC ADDRESS MIGRATION LOG FUNCTION .....	440
<b>33</b>	<b>SPANNING TREE .....</b>	<b>441</b>
<b>33.1</b>	<b>OVERVIEW.....</b>	<b>441</b>
<b>33.2</b>	<b>SPANNING TREE FUNCTION CONFIGURATION .....</b>	<b>445</b>
33.2.1	CONFIGURE BASIC FUNCTIONS OF A SPANNING TREE .....	447
33.2.2	CONFIGURE BRIDGE PROPERTIES.....	450
33.2.3	CONFIGURE SPANNING TREE PORT PROPERTIES .....	453
33.2.4	CONFIGURE THE WORKING MODE OF A SPANNING TREE .....	463
33.2.5	CONFIGURE THE SPANNING TREE PROTECTION FUNCTION .....	464
33.2.6	CONFIGURE THE FUNCTION OF CONFIGURING PSEUDO-INFORMATION OF SPANNING TREE.....	470
33.2.7	SPANNING TREE MONITORING AND MAINTAINING .....	474
<b>33.3</b>	<b>SPANNING TREE TYPICAL CONFIGURATION EXAMPLE .....</b>	<b>475</b>
33.3.1	MSTP TYPICAL APPLICATION .....	475
33.3.2	APPLICATION OF BASIC MSTP FUNCTIONS IN THE MLAG ENVIRONMENT.....	480
<b>34</b>	<b>LOOPBACK DETECTION .....</b>	<b>484</b>

<b>34.1</b>	<b>OVERVIEW</b> .....	<b>484</b>
<b>34.2</b>	<b>LOOPBACK DETECTION FUNCTION CONFIGURATION</b> .....	<b>484</b>
34.2.1	CONFIGURE BASIC FUNCTIONS OF LOOPBACK DETECTION. ....	485
34.2.2	CONFIGURE BASIC PARAMETERS OF LOOPBACK DETECTION.....	486
34.2.3	LOOPBACK DETECTION MONITORING AND MAINTAINING .....	488
<b>34.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF LOOPBACK DETECTION</b> .....	<b>489</b>
34.3.1	CONFIGURE REMOTE LOOPBACK DETECTION .....	489
34.3.2	CONFIGURE LOCAL LOOPBACK DETECTION .....	492
<b>35</b>	<b>ERROR-DISABLE MANAGEMENT</b> .....	<b>496</b>
<b>35.1</b>	<b>OVERVIEW</b> .....	<b>496</b>
<b>35.2</b>	<b>ERROR-DISABLE MANAGEMENT FUNCTION CONFIGURATION</b> .....	<b>496</b>
35.2.1	CONFIGURE ERROR-DISABLE BASIC FUNCTIONS .....	497
35.2.2	CONFIGURE ERROR-DISABLE AUTOMATIC RECOVERY.....	497
35.2.3	ERROR-DISABLE MANAGEMENT MONITORING AND MAINTAINING .....	498
<b>35.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF ERROR-DISABLE MANAGEMENT</b> .....	<b>499</b>
35.3.1	COMBINATION OF ERROR-DISABLE AND STORM SUPPRESSION .....	499
<b>36</b>	<b>GVRP</b> .....	<b>503</b>
<b>36.1</b>	<b>OVERVIEW</b> .....	<b>503</b>
<b>36.2</b>	<b>GVRP FUNCTION CONFIGURATION</b> .....	<b>503</b>
36.2.1	ENABLE GVRP FUNCTION.....	504
36.2.2	CONFIGURE GVRP PORT .....	504
<b>37</b>	<b>MLAG</b> .....	<b>506</b>
<b>37.1</b>	<b>OVERVIEW</b> .....	<b>506</b>
<b>37.2</b>	<b>MLAG FUNCTION CONFIGURATION</b> .....	<b>508</b>
●	<b>MLAG FUNCTION, SUPPORTING SOFTWARE LEARNING INSTEAD OF HARDWARE LEARNING</b> .....	<b>509</b>
37.2.1	CREATE MLAG DOMAIN .....	509
37.2.2	CONFIGURE MLAG PARAMETERS .....	510
37.2.3	CONFIGURE KEEPALIVE PARAMETERS .....	515
37.2.4	CONFIGURE PEER-LINK.....	517
37.2.5	CONFIGURE MLAG PORT .....	517
37.2.6	CONFIGURE ORPHAN-PORT .....	518
37.2.7	MLAG MONITORING AND MAINTAINING.....	519
<b>37.3</b>	<b>TYPICAL MLAG CONFIGURATION EXAMPLE</b> .....	<b>521</b>

37.3.1	CONFIGURE BASIC FUNCTIONS OF MLAG .....	521
37.3.2	CONFIGURE MULTI-LEVEL MLAG FUNCTIONS .....	525
<b>38</b>	<b>VLAN ISOLATION</b> .....	<b>537</b>
<b>38.1</b>	<b>OVERVIEW</b> .....	<b>537</b>
<b>38.2</b>	<b>VLAN ISOLATION FUNCTION CONFIGURATION</b> .....	<b>537</b>
38.2.1	CONFIGURE VLAN ISOLATION .....	537
38.2.2	VLAN ISOLATION MONITORING AND MAINTAINING .....	539
<b>39</b>	<b>ARP</b> .....	<b>539</b>
<b>39.1</b>	<b>OVERVIEW</b> .....	<b>539</b>
<b>39.2</b>	<b>ARP FUNCTION CONFIGURATION</b> .....	<b>539</b>
39.2.1	CONFIGURE BASIC FUNCTIONS OF ARP .....	540
39.2.2	ARP MONITORING AND MAINTAINING .....	545
<b>39.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF ARP</b> .....	<b>546</b>
39.3.1	CONFIGURE ARP PROXY .....	546
39.3.2	CONFIGURE STATIC ARP .....	547
<b>40</b>	<b>IP BASICS</b> .....	<b>549</b>
<b>40.1</b>	<b>OVERVIEW</b> .....	<b>549</b>
<b>40.2</b>	<b>IP BASIC FUNCTION CONFIGURATION</b> .....	<b>549</b>
40.2.1	CONFIGURE AN IP ADDRESS. ....	551
40.2.2	CONFIGURE BASIC FUNCTIONS OF THE IP PROTOCOL .....	553
40.2.3	CONFIGURE BASIC FUNCTIONS OF THE ICMP PROTOCOL. ....	556
40.2.4	CONFIGURE BASIC FUNCTIONS OF THE TCP PROTOCOL .....	559
<b>40.2.5</b>	<b>CONFIGURE TCP PROTOCOL ANTI-ATTACK FUNCTION</b> .....	<b>564</b>
40.2.6	CONFIGURE BASIC FUNCTIONS OF THE UDP PROTOCOL. ....	565
40.2.7	IP BASICS MONITORING AND MAINTAINING .....	568
<b>41</b>	<b>DHCP</b> .....	<b>570</b>
<b>41.1</b>	<b>OVERVIEW</b> .....	<b>570</b>
<b>41.2</b>	<b>DHCP FUNCTION CONFIGURATION</b> .....	<b>571</b>
41.2.1	CONFIGURE A DHCP ADDRESS POOL .....	572
41.2.2	CONFIGURE OTHER PARAMETERS OF A DHCP SERVER. ....	577
41.2.3	CONFIGURE THE FUNCTIONS OF A DHCP CLIENT .....	578
41.2.4	CONFIGURE THE FUNCTION OF A DHCP RELAY .....	580
41.2.5	DHCP MONITORING AND MAINTAINING .....	583

<b>41.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF DHCP .....</b>	<b>584</b>
41.3.1	CONFIGURE A DHCP SERVER TO STATICALLY ALLOCATE IP ADDRESSES .....	584
41.3.2	CONFIGURE A DHCP SERVER TO DYNAMICALLY ALLOCATE IP ADDRESSES .....	586
41.3.3	CONFIGURE A DHCP RELAY .....	588
41.3.4	CONFIGURE THE DHCP RELAY TO SUPPORT OPTION 82.....	590
<b>42</b>	<b>DNS .....</b>	<b>592</b>
<b>42.1</b>	<b>OVERVIEW.....</b>	<b>592</b>
<b>42.2</b>	<b>DNS FUNCTION CONFIGURATION.....</b>	<b>592</b>
42.2.1	CONFIGURE DNS CACHE SPECIFICATIONS. ....	593
42.2.2	CONFIGURE THE DNS CLIENT FUNCTION. ....	594
42.2.3	CONFIGURE DNS PROBE FUNCTION. ....	595
42.2.4	DNS MONITORING AND MAINTAINING .....	596
<b>42.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF DNS.....</b>	<b>596</b>
42.3.1	CONFIGURE STATIC DOMAIN NAME RESOLUTION. ....	596
42.3.2	CONFIGURE DYNAMIC DOMAIN NAME RESOLUTION. ....	597
<b>43</b>	<b>IPV6 BASICS .....</b>	<b>599</b>
<b>43.1</b>	<b>OVERVIEW.....</b>	<b>599</b>
<b>43.2</b>	<b>IPV6 BASIC FUNCTION CONFIGURATION.....</b>	<b>599</b>
43.2.1	CONFIGURE IPV6 ADDRESSES FOR THE PORTS. ....	601
43.2.2	CONFIGURE THE BASIC FUNCTIONS OF IPV6. ....	604
43.2.3	CONFIGURE IPV6 NEIGHBOR DISCOVERY PROTOCOL.....	606
43.2.4	CONFIGURE TO ENABLE THE ND FAST RESPONSE FUNCTION. ....	612
43.2.5	CONFIGURE L3 INTERFACE ND PROXY.....	612
43.2.6	CONFIGURE ICMPV6 FUNCTIONS. ....	613
43.2.7	CONFIGURE TCP ANTI-ATTACK FUNCTION FOR IPV6.....	615
43.2.8	IPV6 BASIC MONITORING AND MAINTAINING .....	616
<b>43.3</b>	<b>BASIC CONFIGURATION EXAMPLE OF IPV6.....</b>	<b>617</b>
43.3.1	CONFIGURE THE IPV6 ADDRESS OF AN INTERFACE .....	617
43.3.2	CONFIGURING IPV6 NEIGHBOR DISCOVERY .....	620
43.3.3	CONFIGURE L3 ND PROXY .....	622
<b>44</b>	<b>DHCPV6 .....</b>	<b>624</b>
<b>44.1</b>	<b>OVERVIEW.....</b>	<b>624</b>
<b>44.2</b>	<b>DHCPV6 FUNCTION CONFIGURATION.....</b>	<b>625</b>

44.2.1	CONFIGURE A DHCPV6 ADDRESS POOL .....	626
44.2.2	CONFIGURE OTHER PARAMETERS OF THE DHCPV6 SERVER.....	629
44.2.3	CONFIGURE THE FUNCTION OF DHCPV6 CLIENT .....	631
44.2.4	CONFIGURE THE FUNCTION OF DHCPV6 RELAY .....	632
44.2.5	DHCPV6 MONITORING AND MAINTAINING .....	634
<b>44.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF DHCPV6.....</b>	<b>635</b>
44.3.1	CONFIGURE THE DHCPV6 SERVER TO STATICALLY ALLOCATE IPV6 ADDRESSES. ....	635
44.3.2	CONFIGURE DHCPV6 SERVER TO DYNAMICALLY ALLOCATE IPV6 ADDRESSES. ....	637
44.3.3	CONFIGURE DHCPV6 RELAY. ....	638
<b>45</b>	<b>GRE .....</b>	<b>640</b>
<b>45.1</b>	<b>OVERVIEW.....</b>	<b>640</b>
<b>45.2</b>	<b>GRE FUNCTION CONFIGURATION.....</b>	<b>641</b>
45.2.1	CONFIGURE GRE TUNNELS. ....	641
45.2.2	GRE MONITORING AND MAINTAINING .....	643
<b>45.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF GRE.....</b>	<b>643</b>
45.3.1	CONFIGURE BASIC FUNCTIONS OF GRE .....	643
45.3.2	CONFIGURE BASIC FUNCTIONS OF GRE OVER IPV6 .....	646
<b>46</b>	<b>IPIP TUNNEL.....</b>	<b>651</b>
<b>46.1</b>	<b>OVERVIEW.....</b>	<b>651</b>
<b>46.2</b>	<b>IPIP FUNCTION CONFIGURATION.....</b>	<b>652</b>
46.2.1	CONFIGURE IPIP TUNNELS. ....	652
46.2.2	IPIP MONITORING AND MAINTAINING .....	654
<b>46.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF IPIP TUNNEL.....</b>	<b>654</b>
46.3.1	CONFIGURE IPIP BASIC FUNCTIONS .....	654
<b>47</b>	<b>TRANSITION TUNNEL.....</b>	<b>657</b>
<b>47.1</b>	<b>OVERVIEW.....</b>	<b>657</b>
<b>47.2</b>	<b>TRANSITION TUNNELS FUNCTION CONFIGURATION.....</b>	<b>659</b>
47.2.1	MANUALLY CONFIGURE IPV6 OVER IPV4 TUNNELS.....	659
47.2.2	CONFIGURE 6TO4 TUNNELS.....	661
47.2.3	CONFIGURE ISATAP TUNNELS .....	663
47.2.4	TRANSITION TUNNEL MONITORING AND MAINTAINING .....	665
<b>47.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF TRANSITION TUNNEL .....</b>	<b>665</b>
47.3.1	CONFIGURE BASIC FUNCTIONS OF MANUALLY CONFIGURED IPV6 OVER IPV4 TUNNELS. ....	665

47.3.2	CONFIGURE BASIC FUNCTIONS OF 6TO4 TUNNELS .....	668
47.3.3	CONFIGURE BASIC FUNCTIONS OF ISATAP TUNNELS .....	672
<b>48</b>	<b>IPV6 TUNNEL .....</b>	<b>676</b>
<b>48.1</b>	<b>OVERVIEW.....</b>	<b>676</b>
<b>48.2</b>	<b>IPV6 TUNNEL FUNCTION CONFIGURATION .....</b>	<b>677</b>
48.2.1	CONFIGURE IPV4 OVER IPV6 TUNNELS.....	677
48.2.2	CONFIGURE IPV6 OVER IPV6 TUNNELS.....	679
48.2.3	IPV6 TUNNEL MONITORING AND MAINTAINING .....	680
<b>48.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF IPV6 TUNNEL .....</b>	<b>680</b>
48.3.1	CONFIGURE BASIC FUNCTIONS OF IPV4 OVER IPV6 .....	680
48.3.2	CONFIGURE BASIC FUNCTIONS OF IPV6 OVER IPV6 .....	684
<b>49</b>	<b>ROUTING BASICS .....</b>	<b>687</b>
<b>49.1</b>	<b>OVERVIEW.....</b>	<b>687</b>
<b>49.2</b>	<b>ROUTING BASIC FUNCTION CONFIGURATION .....</b>	<b>688</b>
49.2.1	CONFIGURE LOAD BALANCING FOR ROUTING.....	688
49.2.2	CONFIGURE THE CAPACITY OF ROUTES FOR VIRTUAL ROUTE FORWARDING (VRF) ROUTES.....	690
49.2.3	ROUTING BASIC MONITORING AND MAINTAINING .....	691
<b>50</b>	<b>IPV6 ROUTING BASICS.....</b>	<b>692</b>
<b>50.1</b>	<b>OVERVIEW.....</b>	<b>692</b>
<b>50.2</b>	<b>IPV6 ROUTING BASIC FUNCTION CONFIGURATION .....</b>	<b>692</b>
50.2.1	CONFIGURE IPV6 ROUTING LOAD BALANCING .....	693
50.2.2	IPV6 ROUTING BASIC MONITORING AND MAINTAINING.....	693
<b>51</b>	<b>STATIC ROUTES .....</b>	<b>695</b>
<b>51.1</b>	<b>OVERVIEW.....</b>	<b>695</b>
<b>51.2</b>	<b>STATIC ROUTING FUNCTION CONFIGURATION .....</b>	<b>696</b>
51.2.1	CONFIGURE A STATIC ROUTE.....	696
51.2.2	CONFIGURE THE DEFAULT ADMINISTRATIVE DISTANCE.....	698
51.2.3	CONFIGURE THE RECURSIVE FUNCTION .....	698
51.2.4	CONFIGURE LOAD BALANCING ROUTES.....	699
51.2.5	CONFIGURE A FLOATING ROUTE .....	700
51.2.6	CONFIGURE A STATIC ROUTE TO COORDINATE WITH BFD.....	701
51.2.7	CONFIGURE A STATIC ROUTE TO COORDINATE WITH TRACK.....	702
51.2.8	CONFIGURE STATIC ROUTE FRR.....	703

51.2.9	STATIC ROUTE MONITORING AND MAINTAINING .....	704
<b>51.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF STATIC ROUTE .....</b>	<b>705</b>
51.3.1	CONFIGURE BASIC FUNCTIONS OF STATIC ROUTE.....	705
51.3.2	CONFIGURE STATIC FLOATING ROUTE .....	706
51.3.3	CONFIGURE STATIC NULL0 INTERFACE ROUTE.....	708
51.3.4	CONFIGURE STATIC RECURSIVE ROUTE .....	710
51.3.5	CONFIGURE A STATIC ROUTE TO COORDINATE WITH BFD.....	712
51.3.6	CONFIGURE STATIC ROUTE FRR.....	714
<b>52</b>	<b>IPV6 STATIC ROUTE .....</b>	<b>717</b>
<b>52.1</b>	<b>OVERVIEW.....</b>	<b>717</b>
<b>52.2</b>	<b>IPV6 STATIC ROUTING FUNCTION CONFIGURATION .....</b>	<b>717</b>
52.2.1	CONFIGURE IPV6 STATIC ROUTE.....	718
52.2.2	CONFIGURE IPV6 LOAD BALANCING ROUTE .....	719
52.2.3	CONFIGURE IPV6 FLOATING ROUTE .....	720
52.2.4	CONFIGURE IPV6 STATIC ROUTE TO COORDINATE WITH TRACK .....	721
52.2.5	CONFIGURE IPV6 STATIC ROUTE FRR .....	722
52.2.6	IPV6 STATIC ROUTE MONITORING AND MAINTAINING .....	723
<b>52.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF IPV6 STATIC ROUTE .....</b>	<b>724</b>
52.3.1	CONFIGURE BASIC FUNCTIONS OF IPV6 STATIC ROUTE .....	724
52.3.2	CONFIGURE IPV6 STATIC FLOATING ROUTE.....	726
52.3.3	CONFIGURE IPV6 STATIC NULL0 INTERFACE ROUTE.....	728
52.3.4	CONFIGURE IPV6 STATIC RECURSIVE ROUTE.....	730
52.3.5	CONFIGURE STATIC FRR FOR IPV6 STATIC ROUTE .....	731
52.3.6	CONFIGURE DYNAMIC FRR FOR IPV6 STATIC ROUTE.....	734
<b>53</b>	<b>RIP .....</b>	<b>737</b>
<b>53.1</b>	<b>OVERVIEW.....</b>	<b>737</b>
<b>53.2</b>	<b>RIP FUNCTION CONFIGURATION.....</b>	<b>737</b>
53.2.1	CONFIGURE RIP BASIC FUNCTIONS .....	738
53.2.2	CONFIGURE RIP ROUTE GENERATION .....	742
53.2.3	CONFIGURE RIP ROUTE CONTROL.....	743
53.2.4	CONFIGURE RIP NETWORK AUTHENTICATION .....	749
53.2.5	CONFIGURE RIP NETWORK OPTIMIZATION .....	750

53.2.6	CONFIGURE RIP TO COORDINATE WITH BFD .....	756
53.2.7	RIP MONITORING AND MAINTAINING .....	757
<b>53.3</b>	<b>RIP TYPICAL CONFIGURATION EXAMPLE .....</b>	<b>758</b>
53.3.1	CONFIGURE RIP VERSION.....	758
53.3.2	CONFIGURE RIP ROUTE REDISTRIBUTION .....	759
53.3.3	CONFIGURE THE RIP METRIC OFFSET .....	762
53.3.4	CONFIGURE RIP ROUTE FILTRATION.....	764
53.3.5	CONFIGURE RIP ROUTE SUMMARIZATION.....	766
53.3.6	CONFIGURE RIP TO COORDINATE WITH BFD .....	769
53.3.7	CONFIGURE AN RIP STANDBY INTERFACE .....	771
53.3.8	CONFIGURE A PASSIVE RIP INTERFACE .....	773
<b>54</b>	<b>RIPNG .....</b>	<b>775</b>
<b>54.1</b>	<b>OVERVIEW.....</b>	<b>775</b>
<b>54.2</b>	<b>RIPNG FUNCTION CONFIGURATION.....</b>	<b>776</b>
54.2.1	CONFIGURE RIPNG BASIC FUNCTIONS .....	777
54.2.2	CONFIGURE RIPNG ROUTE GENERATION.....	777
54.2.3	CONFIGURE RIPNG ROUTE CONTROL.....	779
54.2.4	CONFIGURE RIPNG NETWORK OPTIMIZATION.....	783
54.2.5	CONFIGURE RIPNG TO COORDINATE WITH BFD.....	787
54.2.6	PIM-DM MONITORING AND MAINTAINING.....	788
<b>54.3</b>	<b>RIPNG TYPICAL CONFIGURATION EXAMPLE .....</b>	<b>789</b>
54.3.1	CONFIGURE RIPNG BASIC FUNCTIONS .....	789
54.3.2	CONFIGURE RIPNG ROUTE REDISTRIBUTION .....	790
54.3.3	CONFIGURE RIPNG METRIC OFFSET.....	793
54.3.4	CONFIGURE RIPNG ROUTE FILTRATION.....	796
54.3.5	CONFIGURE RIPNG ROUTE SUMMARIZATION .....	798
54.3.6	CONFIGURE PASSIVE RIPNG INTERFACE.....	800
54.3.7	CONFIGURE RIPNG TO USE IPSEC ENCRYPTION & AUTHENTICATION.....	802
<b>55</b>	<b>OSPF .....</b>	<b>806</b>
<b>55.1</b>	<b>OVERVIEW.....</b>	<b>806</b>
<b>55.2</b>	<b>OSPF FUNCTION CONFIGURATION .....</b>	<b>807</b>
55.2.1	CONFIGURE OSPF BASIC FUNCTIONS.....	809
55.2.2	CONFIGURE OSPF AREA .....	810

55.2.3	CONFIGURE OSPF NETWORK TYPE .....	813
55.2.4	CONFIGURE OSPF NETWORK AUTHENTICATION.....	816
55.2.5	CONFIGURE OSPF ROUTE GENERATION .....	819
55.2.6	CONFIGURE OSPF ROUTE CONTROL .....	822
55.2.7	CONFIGURE OSPF NETWORK OPTIMIZATION .....	829
55.2.8	CONFIGURE OSPF TO COORDINATE WITH BFD .....	836
55.2.9	CONFIGURE OSPF FRR.....	837
55.2.10	CONFIGURE OSPF GR.....	838
55.2.11	OSPF MONITORING AND MAINTAINING .....	840
<b>55.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF OSPF .....</b>	<b>842</b>
55.3.1	CONFIGURE OSPF BASIC FUNCTIONS.....	842
55.3.2	CONFIGURE OSPF AUTHENTICATION .....	846
55.3.3	CONFIGURE OSPF ROUTE REDISTRIBUTION.....	850
55.3.4	CONFIGURE OSPF MULTIPROCESS .....	853
55.3.5	CONFIGURE OSPF EXTERNAL ROUTE SUMMARIZATION .....	858
55.3.6	CONFIGURE OSPF INTER-AREA SUMMARIZATION.....	861
55.3.7	CONFIGURE OSPF INTER-AREA ROUTE FILTRATION.....	866
55.3.8	CONFIGURE OSPF TOTALLY STUB AREA .....	870
55.3.9	CONFIGURE OSPF NSSA .....	872
55.3.10	CONFIGURE OSPF TO COORDINATE WITH BFD .....	876
55.3.11	CONFIGURE OSPF FRR.....	879
<b>56</b>	<b>OSPFV3 .....</b>	<b>883</b>
<b>56.1</b>	<b>OVERVIEW.....</b>	<b>883</b>
<b>56.2</b>	<b>OSPFV3 FUNCTION CONFIGURATION .....</b>	<b>883</b>
56.2.1	CONFIGURE BASIC FUNCTIONS OF OSPFV3 .....	885
56.2.2	CONFIGURE OSPFV3 AREA.....	886
56.2.3	CONFIGURE NETWORK TYPE OF OSPFV3.....	889
56.2.4	CONFIGURE OSPFV3 NETWORK AUTHENTICATION .....	892
56.2.5	CONFIGURE OSPFV3 ROUTE GENERATION.....	893
56.2.6	CONFIGURE OSPFV3 ROUTE CONTROL .....	895
56.2.7	CONFIGURE OSPFV3 NETWORK OPTIMIZATION .....	901
56.2.8	CONFIGURE OSPFV3 FRR .....	906

56.2.9	CONFIGURE OSPFV3 GR .....	907
56.2.10	CONFIGURE COORDINATION OF OSPFV3 WITH BFD .....	909
56.2.11	OSPFV3 MONITORING AND MAINTAINING .....	910
<b>56.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF OSPFV3 .....</b>	<b>911</b>
56.3.1	CONFIGURE BASIC FUNCTIONS OF OSPFV3 .....	911
56.3.2	CONFIGURE OSPFV3 TO USE IPSEC ENCRYPTION & AUTHENTICATION .....	916
56.3.3	CONFIGURE COORDINATION OF OSPFV3 WITH BFD.....	924
56.3.4	CONFIGURE OSPFV3 STATIC FRR.....	927
56.3.5	CONFIGURE OSPFV3 DYNAMIC FRR .....	930
<b>57</b>	<b>IS-IS.....</b>	<b>933</b>
<b>57.1</b>	<b>OVERVIEW.....</b>	<b>933</b>
<b>57.2</b>	<b>IS-IS FUNCTION CONFIGURATION.....</b>	<b>934</b>
57.2.1	CONFIGURE BASIC FUNCTIONS OF IS-IS .....	935
57.2.2	CONFIGURE ATTRIBUTES OF IS-IS LAYER .....	937
57.2.3	CONFIGURE IS-IS ROUTE GENERATION .....	938
57.2.4	CONFIGURE IS-IS ROUTE CONTROL .....	940
57.2.5	CONFIGURE IS-IS NETWORK OPTIMIZATION .....	944
57.2.6	CONFIGURE IS-IS NETWORK AUTHENTICATION .....	954
57.2.7	CONFIGURE COORDINATION OF IS-IS WITH BFD.....	955
57.2.8	CONFIGURE IS-IS FRR.....	956
57.2.9	CONFIGURE IS-IS GR.....	957
57.2.10	IS-IS MONITORING AND MAINTAINING .....	959
<b>57.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF IS-IS.....</b>	<b>960</b>
57.3.1	CONFIGURE BASIC FUNCTIONS OF IS-IS .....	960
57.3.2	CONFIGURE THE DIS ELECTION OF IS-IS .....	963
57.3.3	CONFIGURE IS-IS INTER-AREA ROUTE LEAK .....	966
57.3.4	IS-IS ROUTE REDISTRIBUTION.....	970
57.3.5	CONFIGURE IS-IS NEIGHBOR AUTHENTICATION .....	973
57.3.6	CONFIGURE COORDINATION OF IS-IS WITH BFD.....	977
57.3.7	CONFIGURE ISIS FRR .....	979
<b>58</b>	<b>IPV6 IS-IS.....</b>	<b>983</b>
<b>58.1</b>	<b>OVERVIEW.....</b>	<b>983</b>
<b>58.2</b>	<b>IPV6 IS-IS FUNCTION CONFIGURATION .....</b>	<b>983</b>

58.2.1	CONFIGURE BASIC FUNCTIONS OF IPV6 IS-IS .....	984
58.2.2	CONFIGURE ATTRIBUTES OF IPV6 IS-IS LAYER.....	986
58.2.3	CONFIGURE IPV6 IS-IS ROUTE GENERATION .....	987
58.2.4	CONFIGURE IPV6 IS-IS ROUTE CONTROL.....	989
58.2.5	CONFIGURE IPV6 IS-IS NETWORK OPTIMIZATION.....	993
58.2.6	CONFIGURE IPV6 IS-IS NETWORK AUTHENTICATION .....	1003
58.2.7	CONFIGURE IPV6 IS-IS FRR .....	1004
58.2.8	CONFIGURE IPV6 IS-IS GR .....	1006
58.2.9	IPV6 IS-IS MONITORING AND MAINTAINING .....	1007
<b>58.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF IS-ISV6 .....</b>	<b>1008</b>
58.3.1	CONFIGURE BASIC FUNCTIONS OF IS-ISV6 .....	1008
58.3.2	CONFIGURE IPV6 IS-IS STATIC FRR.....	1013
58.3.3	CONFIGURE IPV6 IS-IS DYNAMIC FRR.....	1016
<b>59</b>	<b>IRMP.....</b>	<b>1019</b>
<b>59.1</b>	<b>OVERVIEW.....</b>	<b>1019</b>
<b>59.2</b>	<b>IRMP FUNCTION CONFIGURATION.....</b>	<b>1019</b>
59.2.1	CONFIGURE BASIC FUNCTIONS OF IRMP.....	1020
59.2.2	CONFIGURE IRMP ROUTE GENERATION.....	1021
59.2.3	CONFIGURE IRMP ROUTE CONTROL .....	1022
59.2.4	CONFIGURE IRMP NETWORK OPTIMIZATION .....	1028
59.2.5	CONFIGURE IRMP NETWORK AUTHENTICATION.....	1032
59.2.6	IRMP MONITORING AND MAINTAINING.....	1033
<b>59.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF IRMP .....</b>	<b>1034</b>
59.3.1	CONFIGURE BASIC FUNCTIONS OF IRMP.....	1034
59.3.2	CONFIGURE IRMP ROUTE REDISTRIBUTION .....	1035
59.3.3	CONFIGURE IRMP METRIC OFFSET .....	1038
59.3.4	CONFIGURE IRMP ROUTE FILTRATION .....	1041
59.3.5	CONFIGURE IRMP ROUTE SUMMARIZATION .....	1044
59.3.6	CONFIGURE IRMP LOAD BALANCING .....	1047
<b>60</b>	<b>BGP .....</b>	<b>1051</b>
<b>60.1</b>	<b>OVERVIEW.....</b>	<b>1051</b>
<b>60.2</b>	<b>BGP FUNCTION CONFIGURATION .....</b>	<b>1051</b>

60.2.1	CONFIGURE BGP NEIGHBOR.....	1053
60.2.2	CONFIGURE BGP ROUTE GENERATION.....	1060
60.2.3	CONFIGURE BGP ROUTE CONTROL .....	1062
60.2.4	CONFIGURE BGP ROUTE ATTRIBUTES.....	1068
60.2.5	CONFIGURE BGP NETWORK OPTIMIZATION.....	1078
60.2.6	CONFIGURE LARGE BGP NETWORK .....	1084
60.2.7	CONFIGURE BGP GR.....	1087
60.2.8	CONFIGURE BGP TO COORDINATE WITH BFD.....	1089
60.2.9	CONFIGURE BGP FRR.....	1091
60.2.10	CONFIGURE BGP LS .....	1092
60.2.11	BGP MONITORING AND MAINTAINING.....	1093
<b>60.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF BGP .....</b>	<b>1095</b>
60.3.1	CONFIGURE BASIC FUNCTIONS OF BGP .....	1095
60.3.2	CONFIGURE BGP ROUTE REDISTRIBUTION .....	1098
60.3.3	CONFIGURE COMMUNITY ATTRIBUTES OF BGP.....	1100
60.3.4	CONFIGURE BGP ROUTE REFLECTOR.....	1103
60.3.5	CONFIGURE BGP ROUTE AGGREGATION .....	1107
60.3.6	CONFIGURE BGP ROUTE PREFERENCE .....	1110
60.3.7	CONFIGURE BGP CONFEDERATION.....	1116
60.3.8	CONFIGURE BGP TO COORDINATE WITH BFD.....	1121
60.3.9	CONFIGURE BGP FRR.....	1126
60.3.10	CONFIGURE BASIC FUNCTIONS OF BGP-LS .....	1129
<b>61</b>	<b>IPV6 BGP .....</b>	<b>1134</b>
<b>61.1</b>	<b>OVERVIEW.....</b>	<b>1134</b>
<b>61.2</b>	<b>IPV6 BGP FUNCTION CONFIGURATION .....</b>	<b>1135</b>
61.2.1	CONFIGURE IPV6 BGP NEIGHBOR .....	1136
61.2.2	CONFIGURE IPV6 BGP ROUTE GENERATION .....	1142
61.2.3	CONFIGURE IPV6 BGP ROUTE CONTROL .....	1145
61.2.4	CONFIGURE IPV6 BGP ROUTE ATTRIBUTES .....	1151
61.2.5	CONFIGURE IPV6 BGP NETWORK OPTIMIZATION .....	1162
61.2.6	CONFIGURE LARGE IPV6 BGP NETWORK .....	1167
61.2.7	CONFIGURE IPV6 BGP GR.....	1170
61.2.8	CONFIGURE COORDINATION OF IPV6 BGP WITH BFD .....	1173

61.2.9	CONFIGURE IPV6 BGP FRR.....	1175
61.2.10	IPV6 BGP MONITORING AND MAINTAINING.....	1176
<b>61.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF IPV6 BGP.....</b>	<b>1178</b>
61.3.1	CONFIGURE BASIC FUNCTIONS OF IPV6 BGP.....	1178
61.3.2	CONFIGURE IPV6 BGP ROUTE REDISTRIBUTION.....	1182
61.3.3	CONFIGURE IPV6 BGP COMMUNITY ATTRIBUTES.....	1185
61.3.4	CONFIGURE IPV6 BGP ROUTE REFLECTOR.....	1188
61.3.5	CONFIGURE IPV6 BGP ROUTE AGGREGATION.....	1193
61.3.6	CONFIGURE IPV6 BGP ROUTE PREFERENCE.....	1197
61.3.7	CONFIGURE COORDINATION OF IPV6 BGP WITH BFD.....	1205
61.3.8	CONFIGURE IPV6 BGP STATIC FRR.....	1211
61.3.9	CONFIGURE IPV6 BGP DYNAMIC FRR.....	1214
<b>62</b>	<b>POLICY ROUTE.....</b>	<b>1217</b>
<b>62.1</b>	<b>OVERVIEW.....</b>	<b>1217</b>
<b>62.2</b>	<b>FUNCTION CONFIGURATION OF POLICY ROUTE.....</b>	<b>1217</b>
62.2.1	CONFIGURE POLICY ROUTE.....	1218
62.2.2	CONFIGURATION APPLICATION OF POLICY ROUTE.....	1223
62.2.3	POLICY ROUTE MONITORING AND MAINTAINING.....	1227
<b>62.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF POLICY ROUTE.....</b>	<b>1228</b>
62.3.1	CONFIGURE POLICY ROUTE.....	1228
<b>63</b>	<b>ROUTING POLICY TOOL.....</b>	<b>1232</b>
<b>63.1</b>	<b>OVERVIEW.....</b>	<b>1232</b>
<b>63.2</b>	<b>FUNCTION CONFIGURATION OF ROUTING POLICY TOOL.....</b>	<b>1232</b>
63.2.1	CONFIGURE PREFIX LIST.....	1233
63.2.2	CONFIGURE AS-PATH LIST.....	1234
63.2.3	CONFIGURE LIST OF COMMUNITY ATTRIBUTES.....	1236
63.2.4	CONFIGURE LIST OF EXTCOMMUNITY ATTRIBUTES.....	1237
63.2.5	CONFIGURE ROUTING MAP.....	1238
63.2.6	CONFIGURE KEY-CHAIN.....	1244
63.2.7	ROUTING POLICY TOOL MONITORING AND MAINTAINING.....	1245
<b>63.3</b>	<b>EXAMPLE OF TYPICAL ROUTING POLICY TOOL CONFIGURATION.....</b>	<b>1246</b>
63.3.1	CONFIGURE ROUTE REDISTRIBUTION AND ASSOCIATE ROUTING POLICY.....	1246

63.3.2	CONFIGURE BGP TO ASSOCIATE WITH THE ROUTING POLICY .....	1250
<b>64</b>	<b>L2 MULTICAST BASICS .....</b>	<b>1258</b>
<b>64.1</b>	<b>OVERVIEW.....</b>	<b>1258</b>
<b>64.2</b>	<b>L2 MULTICAST BASICS FUNCTION CONFIGURATION.....</b>	<b>1258</b>
64.2.1	CONFIGURE UNKNOWN PACKET FORWARDING POLICY OF L2 MULTICAST .....	1259
64.2.2	CONFIGURE L2 STATIC MULTICAST .....	1262
64.2.3	MONITORING AND MAINTAINING OF L2 MULTICAST BASICS .....	1263
<b>64.3</b>	<b>TYPICAL CONFIGURATION EXAMPLES OF L2 STATIC MULTICAST .....</b>	<b>1263</b>
64.3.1	CONFIGURE L2 STATIC MULTICAST .....	1263
64.3.2	CONFIGURE IPV6 L2 STATIC MULTICAST.....	1266
<b>65</b>	<b>IGMP SNOOPING .....</b>	<b>1269</b>
<b>65.1</b>	<b>OVERVIEW.....</b>	<b>1269</b>
<b>65.2</b>	<b>IGMP SNOOPING FUNCTION CONFIGURATION .....</b>	<b>1269</b>
65.2.1	CONFIGURE THE BASIC FUNCTIONS OF IGMP SNOOPING .....	1270
65.2.2	CONFIGURE IGMP SNOOPING QUERIER.....	1272
65.2.3	CONFIGURE IGMP SNOOPING ROUTER PORT.....	1276
65.2.4	CONFIGURE THE IGMP SNOOPING TCN EVENT .....	1277
65.2.5	CONFIGURE THE IGMP SNOOPING POLICY.....	1279
65.2.6	CONFIGURE IGMP SNOOPING PROXY .....	1283
65.2.7	CONFIGURE IGMP SNOOPING STATIC GROUP .....	1284
65.2.8	MONITORING AND MAINTAINING OF IGMP SNOOPING .....	1284
<b>65.3</b>	<b>TYPICAL CONFIGURATION EXAMPLES OF IGMP SNOOPING .....</b>	<b>1286</b>
65.3.1	CONFIGURE IGMP SNOOPING .....	1286
65.3.2	CONFIGURE MULTICAST RECEIVING CONTROL .....	1288
65.3.3	CONFIGURE IGMP SNOOPING PROXY .....	1291
65.3.4	CONFIGURE UNKNOWN MULTICAST REDIRECTION .....	1295
65.3.5	CONFIGURE IGMP SNOOPING STATIC GROUP .....	1297
<b>66</b>	<b>MULTICAST VLAN.....</b>	<b>1299</b>
<b>66.1</b>	<b>OVERVIEW.....</b>	<b>1299</b>
<b>66.2</b>	<b>MULTICAST VLAN CONFIGURATION .....</b>	<b>1299</b>
66.2.1	CONFIGURE MVP .....	1299
66.2.2	CONFIGURE MVR.....	1301
66.2.3	MONITORING AND MAINTAINING OF MULTICAST VLAN .....	1302

<b>66.3</b>	<b>TYPICAL CONFIGURATION EXAMPLES OF MULTICAST VLAN .....</b>	<b>1302</b>
66.3.1	CONFIGURE MVP .....	1302
66.3.2	CONFIGURE MVR.....	1305
<b>67</b>	<b>IPV4 MULTICAST BASICS .....</b>	<b>1309</b>
<b>67.1</b>	<b>OVERVIEW.....</b>	<b>1309</b>
<b>67.2</b>	<b>IPv4 MULTICAST BASICS FUNCTION CONFIGURATION .....</b>	<b>1309</b>
67.2.1	ENABLE IP MULTICAST FORWARDING.....	1309
67.2.2	CONFIGURE IP MULTICAST FORWARDING RULES.....	1310
<b>68</b>	<b>IGMP .....</b>	<b>1313</b>
<b>68.1</b>	<b>OVERVIEW.....</b>	<b>1313</b>
<b>68.2</b>	<b>IGMP FUNCTION CONFIGURATION.....</b>	<b>1313</b>
68.2.1	CONFIGURE BASIC IGMP FUNCTIONS .....	1314
68.2.2	ADJUST AND OPTIMIZE IGMP NETWORK .....	1318
68.2.3	CONFIGURE IGMP SSM MAPPING.....	1322
68.2.4	IGMP MONITORING AND MAINTAINING .....	1323
<b>68.3</b>	<b>IGMP TYPICAL CONFIGURATION EXAMPLE.....</b>	<b>1324</b>
68.3.1	CONFIGURE IGMP.....	1324
68.3.2	CONFIGURE IGMP SSM MAPPING.....	1327
68.3.3	CONFIGURE IGMP STATIC GROUP JOINING .....	1333
68.3.4	CONFIGURE IGMP MULTICAST GROUP FILTERING.....	1336
<b>69</b>	<b>PIM-DM.....</b>	<b>1341</b>
<b>69.1</b>	<b>OVERVIEW.....</b>	<b>1341</b>
<b>69.2</b>	<b>PIM-DM FUNCTION CONFIGURATION.....</b>	<b>1341</b>
69.2.1	CONFIGURE BASIC FUNCTIONS OF PIM-DM .....	1342
69.2.2	CONFIGURE PIM-DM NEIGHBORS .....	1343
69.2.3	CONFIGURE STATE REFRESH PARAMETERS .....	1345
69.2.4	PIM-DM MONITORING AND MAINTAINING .....	1346
<b>69.3</b>	<b>PIM-DM TYPICAL CONFIGURATION EXAMPLE .....</b>	<b>1347</b>
69.3.1	CONFIGURE BASIC FUNCTIONS OF PIM-DM .....	1347
<b>70</b>	<b>PIM-SM .....</b>	<b>1352</b>
<b>70.1</b>	<b>OVERVIEW.....</b>	<b>1352</b>
<b>70.2</b>	<b>PIM-SM FUNCTION CONFIGURATION .....</b>	<b>1352</b>
70.2.1	CONFIGURE BASIC FUNCTIONS OF PIM-SM.....	1354

70.2.2	CONFIGURE PIM-SM AGGREGATION ROUTER.....	1355
70.2.3	CONFIGURE PIM-SM BOOTSTRAP ROUTER.....	1357
70.2.4	CONFIGURE PIM-SM MULTICAST SOURCE REGISTRATION.....	1358
70.2.5	CONFIGURE PIM-SM NEIGHBOR PARAMETERS.....	1362
70.2.6	CONFIGURE PIM-SM SPT SWITCHING.....	1365
70.2.7	CONFIGURE PIM-SSM .....	1366
<b>70.2.8</b>	<b>CONFIGURE ADAPTIVE BASIC FUNCTIONS OF PIM .....</b>	<b>1367</b>
70.2.9	CONFIGURE PIM-SM CONTROL POLICY .....	1368
70.2.10	CONFIGURE PIM-SM SUPPORT (*, *, RP).....	1369
70.2.11	CONFIGURE PIM-SM BFD.....	1370
70.2.12	PIM-SM MONITORING AND MAINTAINING.....	1371
<b>70.3</b>	<b>PIM-SM TYPICAL CONFIGURATION EXAMPLE.....</b>	<b>1372</b>
70.3.1	CONFIGURE BASIC FUNCTIONS OF PIM-SM.....	1372
70.3.2	CONFIGURE PIM-SSM .....	1382
70.3.3	CONFIGURE PIM-SM MULTICAST FORWARDING CONTROL .....	1388
70.3.4	CONFIGURE DR SWITCHING CONVERGENCE WITH PIM-SM AND BFD LINKAGE.....	1398
70.3.5	CONFIGURE RPF ROUTING SWITCHING CONVERGENCE WITH PIM-SM AND BFD LINKAGE ..	1409
<b>71</b>	<b>MSDP.....</b>	<b>1420</b>
<b>71.1</b>	<b>OVERVIEW.....</b>	<b>1420</b>
<b>71.2</b>	<b>MSDP FUNCTION CONFIGURATION .....</b>	<b>1420</b>
71.2.1	CONFIGURE MSDP PEER.....	1421
71.2.2	CONFIGURE MSDP PEER CONNECTION .....	1423
71.2.3	CONFIGURE SA PACKET .....	1424
71.2.4	MSDP MONITORING AND MAINTAINING .....	1426
<b>71.3</b>	<b>MSDP TYPICAL CONFIGURATION EXAMPLE .....</b>	<b>1427</b>
71.3.1	CONFIGURE PIM-SM INTER-DOMAIN MULTICAST .....	1427
71.3.2	CONFIGURE ANYCAST RP .....	1440
<b>72</b>	<b>MLD .....</b>	<b>1454</b>
<b>72.1</b>	<b>OVERVIEW.....</b>	<b>1454</b>
<b>72.2</b>	<b>MLD FUNCTION CONFIGURATION .....</b>	<b>1454</b>
72.2.1	CONFIGURE BASIC FUNCTIONS OF MLD .....	1454
72.2.2	ADJUST AND OPTIMIZE MLD NETWORK .....	1457
72.2.3	CONFIGURE MLD SSM MAPPING.....	1461

72.2.4	MLD MONITORING AND MAINTAINING .....	1463
<b>72.3</b>	<b>MLD TYPICAL CONFIGURATION EXAMPLE .....</b>	<b>1463</b>
72.3.1	CONFIGURE BASIC FUNCTIONS OF MLD .....	1463
72.3.2	CONFIGURE MLD STATIC GROUP JOINING.....	1466
72.3.3	CONFIGURE MLD SSM MAPPING .....	1469
72.3.4	CONFIGURE MLD MULTICAST GROUP FILTERING .....	1476
<b>73</b>	<b>MLD SNOOPING .....</b>	<b>1481</b>
<b>73.1</b>	<b>OVERVIEW.....</b>	<b>1481</b>
<b>73.2</b>	<b>MLD SNOOPING FUNCTION CONFIGURATION.....</b>	<b>1481</b>
73.2.1	CONFIGURE BASIC FUNCTIONS OF MLD SNOOPING .....	1482
73.2.2	CONFIGURE MLD SNOOPING QUERIER.....	1484
73.2.3	CONFIGURE MLD SNOOPING ROUTER PORT.....	1488
73.2.4	CONFIGURE MLD SNOOPING TCN EVENT .....	1490
<b>73.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF MLD SNOOPING.....</b>	<b>1491</b>
73.3.1	CONFIGURE MLD SNOOPING.....	1491
<b>74</b>	<b>IPv6 MULTICAST BASICS .....</b>	<b>1494</b>
<b>74.1</b>	<b>OVERVIEW.....</b>	<b>1494</b>
<b>74.2</b>	<b>IPv6 MULTICAST BASICS FUNCTION CONFIGURATION .....</b>	<b>1494</b>
74.2.1	ENABLE IPv6 MULTICAST FORWARDING .....	1494
74.2.2	CONFIGURE IPv6 MULTICAST FORWARDING RULES .....	1495
74.2.3	MONITORING AND MAINTAINING OF IPv6 MULTICAST BASICS.....	1496
<b>75</b>	<b>IPv6 PIM-SM .....</b>	<b>1497</b>
<b>75.1</b>	<b>OVERVIEW.....</b>	<b>1497</b>
<b>75.2</b>	<b>IPv6 PIM-SM FUNCTION CONFIGURATION .....</b>	<b>1497</b>
75.2.1	CONFIGURE BASIC FUNCTIONS OF IPv6 PIM-SM .....	1498
75.2.2	CONFIGURE IPv6 PIM-SM AGGREGATION ROUTER.....	1499
75.2.3	CONFIGURE IPv6 PIM-SM BOOTSTRAP ROUTER .....	1501
75.2.4	CONFIGURE IPv6 PIM-SM MULTICAST SOURCE REGISTRATION .....	1503
75.2.5	CONFIGURE IPv6 PIM-SM NEIGHBOR PARAMETERS .....	1506
75.2.6	CONFIGURE IPv6 PIM-SM SPT SWITCHING .....	1509
75.2.7	CONFIGURE IPv6 PIM-SSM.....	1510
75.2.8	MONITORING AND MAINTAINING OF IPv6 PIM-SM .....	1511
<b>75.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF IPv6 PIM-SM .....</b>	<b>1512</b>

75.3.1	CONFIGURE BASIC FUNCTIONS OF IPV6 PIM-SM .....	1512
75.3.2	CONFIGURE IPV6 PIM-SSM.....	1523
75.3.3	CONFIGURE IPV6 PIM-SM MULTICAST FORWARDING CONTROL.....	1531
<b>76</b>	<b>HARDWARE QOS.....</b>	<b>1541</b>
<b>76.1</b>	<b>OVERVIEW.....</b>	<b>1542</b>
76.1.1	BACKGROUND .....	1542
76.1.2	SERVICE MODEL.....	1542
76.1.3	INTRODUCTION TO QOS FUNCTIONS.....	1543
<b>76.2</b>	<b>HARDWARE QOS FUNCTION CONFIGURATION.....</b>	<b>1547</b>
76.2.1	CONFIGURE PRIORITY MAPPING .....	1548
76.2.2	CONFIGURE FLOW CLASSIFICATION.....	1550
76.2.3	CONFIGURE TRAFFIC MONITORING .....	1557
76.2.4	CONFIGURE TRAFFIC SHAPING.....	1558
76.2.5	CONFIGURE CONGESTION MANAGEMENT .....	1560
76.2.6	CONFIGURE CONGESTION AVOIDANCE.....	1561
76.2.7	CONFIGURE VFP ACTION GROUP .....	1562
76.2.8	CONFIGURE EXPLICIT CONGESTION NOTIFICATION .....	1565
76.2.9	CONFIGURE TRAFFIC FLOODING .....	1565
76.2.10	HARDWARE QOS MONITORING AND MAINTAINING.....	1566
<b>76.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF HARDWARE QOS.....</b>	<b>1567</b>
76.3.1	CONFIGURE PRIORITY MAPPING .....	1567
76.3.2	CONFIGURE REMARKING .....	1569
76.3.3	CONFIGURE TRAFFIC SHAPING.....	1572
76.3.4	CONFIGURE RATE LIMITING.....	1575
76.3.5	CONFIGURE WRED.....	1577
76.3.6	CONFIGURE SP .....	1579
76.3.7	CONFIGURE WDRR.....	1582
76.3.8	CONFIGURE SP+WDRR.....	1585
76.3.9	CONFIGURE FLOW MIRROR.....	1589
<b>77</b>	<b>MPLS BASICS.....</b>	<b>1591</b>
<b>77.1</b>	<b>OVERVIEW.....</b>	<b>1591</b>
<b>77.2</b>	<b>MPLS BASIC FUNCTION CONFIGURATION.....</b>	<b>1594</b>
77.2.1	CONFIGURE BASIC FUNCTIONS OF MPLS.....	1594

77.2.2	CONFIGURE MPLS FORWARDING CONTROL.....	1596
77.2.3	MPLS BASIC MONITORING AND MAINTAINING.....	1598
<b>78</b>	<b>MPLS LDP.....</b>	<b>1599</b>
<b>78.1</b>	<b>OVERVIEW.....</b>	<b>1599</b>
<b>78.2</b>	<b>MPLS LDP FUNCTION CONFIGURATION.....</b>	<b>1599</b>
78.2.1	CONFIGURE BASIC FUNCTIONS OF LDP.....	1600
78.2.2	CONFIGURE LDP NEIGHBOR PARAMETERS.....	1601
78.2.3	CONFIGURE LDP MD5 AUTHENTICATION.....	1605
78.2.4	CONFIGURE LDP CONTROL ATTRIBUTES.....	1605
78.2.5	CONFIGURE LDP GR.....	1612
78.2.6	CONFIGURE LDP TO COORDINATE WITH BFD.....	1614
78.2.7	LDP MONITORING AND MAINTAINING.....	1616
<b>78.3</b>	<b>MPLS LDP TYPICAL CONFIGURATION EXAMPLE.....</b>	<b>1618</b>
78.3.1	CONFIGURE BASIC FUNCTIONS OF LDP.....	1618
78.3.2	CONFIGURING LDP REMOTE SESSIONS.....	1622
78.3.3	CONFIGURE TO ENABLE COORDINATION BETWEEN MPLS LDP AND BFD.....	1626
<b>79</b>	<b>MPLS L3VPN.....</b>	<b>1633</b>
<b>79.1</b>	<b>OVERVIEW.....</b>	<b>1633</b>
<b>79.2</b>	<b>MPLS L3VPN FUNCTION CONFIGURATION.....</b>	<b>1634</b>
79.2.1	CONFIGURE BASIC FUNCTIONS OF VPN.....	1634
79.2.2	CONFIGURE M-VRF.....	1643
79.2.3	CONFIGURE VPN ROUTE LABEL ASSIGNMENT.....	1647
79.2.4	CONFIGURE VPN TO CROSS DOMAIN.....	1648
79.2.5	CONFIGURE VPN USERS TO ACCESS THE INTERNET.....	1651
79.2.6	CONFIGURE AS OVERRIDE.....	1654
79.2.7	CONFIGURE OSPF PSEUDO-CONNECTIONS.....	1655
79.2.8	MPLS L3VPN MONITORING AND MAINTAINING.....	1658
<b>79.3</b>	<b>MPLS L3VPN TYPICAL CONFIGURATION EXAMPLE.....</b>	<b>1659</b>
79.3.1	CONFIGURE INTRA-DOMAIN MPLS L3VPN.....	1659
79.3.2	CONFIGURE M-VRF.....	1671
79.3.3	CONFIGURE CROSS-DOMAIN OPTION-A.....	1684
79.3.4	CONFIGURE CROSS-DOMAIN OPTIONB.....	1697

79.3.5	CONFIGURE THE AS REPLACEMENT FUNCTION OF BGP.....	1708
79.3.6	CONFIGURE OSPF PSEUDO-CONNECTIONS.....	1721
79.3.7	INTRANET ACCESS TO THE INTERNET .....	1733
79.3.8	SERVICE PROVIDER NETWORK ACCESS TO THE INTERNET WAY .....	1745
79.3.9	CONFIGURE A SHARED VPN.....	1757
<b>80</b>	<b>MPLS OAM .....</b>	<b>1769</b>
<b>80.1</b>	<b>MPLS OAM INTRODUCTION.....</b>	<b>1769</b>
<b>80.2</b>	<b>MPLS OAM FUNCTION CONFIGURATION.....</b>	<b>1769</b>
80.2.1	CONFIGURE THE MPLS OAM FUNCTION. ....	1769
80.2.2	CHECK LSP .....	1770
<b>80.3</b>	<b>MPLS OAM TYPICAL CONFIGURATION EXAMPLE .....</b>	<b>1777</b>
80.3.1	CONFIGURE LSP PING .....	1777
80.3.2	CONFIGURE LSP TRACEROUTE .....	1780
<b>81</b>	<b>ARP CHECK .....</b>	<b>1782</b>
<b>81.1</b>	<b>OVERVIEW.....</b>	<b>1782</b>
<b>81.2</b>	<b>ARP CHECK FUNCTION CONFIGURATION .....</b>	<b>1783</b>
81.2.1	ENABLE ARP CHECK FUNCTION OF THE PORT .....	1783
81.2.2	CONFIGURE BINDING STATIC ENTRIES OF ARP CHECK.....	1784
81.2.3	CONFIGURE TO REINSTALL THE ARP CHECK ENTRIES FAILED IN WRITING HARDWARE.....	1785
81.2.4	ARP CHECK MONITORING AND MAINTAINING .....	1786
<b>81.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF ARP CHECK.....</b>	<b>1786</b>
81.3.1	CONFIGURE BASIC FUNCTIONS OF ARP CHECK .....	1786
81.3.2	COMBINATION OF ARP CHECK WITH DHCP SNOOPING .....	1788
81.3.3	COMBINATION OF ARP CHECK WITH 802.1X.....	1790
<b>82</b>	<b>CPU PROTECTION.....</b>	<b>1793</b>
<b>82.1</b>	<b>OVERVIEW.....</b>	<b>1793</b>
<b>82.2</b>	<b>CONFIGURE CPU PROTECTION FUNCTION .....</b>	<b>1794</b>
82.2.1	CONFIGURE CPU QUEUE OF PROTOCOL PACKETS.....	1794
82.2.2	CONFIGURE THE TRAFFIC RATE LIMITATION OF PROTOCOL PACKETS .....	1795
<b>82.2.3</b>	<b>CONFIGURE TOTAL RATE LIMITATION OF ALL CPU QUEUES .....</b>	<b>1795</b>
82.2.4	CONFIGURE RATE LIMITATION OF EACH CPU QUEUE .....	1796
82.2.5	MAKE USERS' CUSTOM PROTOCOL PACKETS DELIVERED TO CPU FOR PROCESSING .....	1797
82.2.6	CPU PROTECTION MONITORING AND MAINTAINING.....	1799

<b>82.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF CPU PROTECTION .....</b>	<b>1799</b>
82.3.1	CONFIGURE BASIC FUNCTIONS OF CPU PROTECTION .....	1799
82.3.2	CONFIGURE CUSTOM RULES OF CPU PROTECTION .....	1802
<b>83</b>	<b>PORT SECURITY .....</b>	<b>1804</b>
<b>83.1</b>	<b>OVERVIEW.....</b>	<b>1804</b>
83.1.1	INTRODUCTION.....	1804
83.1.2	PORT SECURITY RULES .....	1804
83.1.3	WORKING PRINCIPLE OF PORT SECURITY .....	1805
<b>83.2</b>	<b>PORT SECURITY FUNCTION CONFIGURATION .....</b>	<b>1805</b>
83.2.1	CONFIGURE BASIC FUNCTIONS OF PORT SECURITY.....	1806
83.2.2	CONFIGURE PORT SECURITY RULES.....	1807
83.2.3	CONFIGURE STICKY RULES LEARNING MODE.....	1814
83.2.4	CONFIGURE STATIC MAC ADDRESS AGING FUNCTION .....	1815
83.2.5	CONFIGURE PROCESSING MODE AFTER RECEIVING ILLEGAL PACKETS .....	1816
83.2.6	CONFIGURE LOG SENDING INTERVAL AFTER RECEIVING ILLEGAL PACKETS.....	1817
83.2.7	CONFIGURE PORT SECURITY TO USE ACL FUNCTION .....	1818
83.2.8	PORT SECURITY MONITORING AND MAINTAINING.....	1819
<b>83.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF PORT SECURITY .....</b>	<b>1820</b>
83.3.1	CONFIGURE MAC AND IP RULES FOR PORT SECURITY .....	1820
83.3.2	CONFIGURE MAX RULES FOR PORT SECURITY .....	1821
83.3.3	CONFIGURE STICKY RULES FOR PORT SECURITY .....	1823
<b>84</b>	<b>IP SOURCE GUARD .....</b>	<b>1825</b>
<b>84.1</b>	<b>OVERVIEW.....</b>	<b>1825</b>
<b>84.2</b>	<b>IP SOURCE GUARD FUNCTION CONFIGURATION .....</b>	<b>1826</b>
84.2.1	CONFIGURE STATIC BINDING ENTRIES FOR PORT IP SOURCE GUARD .....	1826
84.2.2	CONFIGURE THE PORT IP SOURCE GUARD FUNCTION .....	1827
84.2.3	CONFIGURE PORT IP SOURCE GUARD TO FILTER PACKET TYPE.....	1829
84.2.4	CONFIGURE THE FUNCTION OF BINDING STATIC ENTRIES OF PORT MAC.....	1830
84.2.5	CONFIGURE GLOBAL IP SOURCE GUARD FUNCTION .....	1831
84.2.6	IP SOURCE GUARD MONITORING AND MAINTAINING .....	1832
<b>84.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF IP SOURCE GUARD .....</b>	<b>1833</b>
84.3.1	CONFIGURE VALID PORT IP SOURCE GUARD FUNCTION BASED ON DYNAMIC ENTRIES OF DHCP SNOOPING.....	1833

84.3.2	CONFIGURE THE PORT IP SOURCE GUARD FUNCTION WHICH TAKES EFFECT BASED ON STATIC ENTRIES.....	1835
<b>85</b>	<b>IPV6 SOURCE GUARD</b> .....	<b>1838</b>
<b>85.1</b>	<b>OVERVIEW</b> .....	<b>1838</b>
<b>85.2</b>	<b>IPV6 SOURCE GUARD FUNCTION CONFIGURATION</b> .....	<b>1838</b>
85.2.1	ENABLE PORT IPV6 SOURCE GUARD FUNCTION.....	1839
85.2.2	CONFIGURE NUMBER OF BINDING ENTRIES OF PORT IPV6 SOURCE GUARD .....	1840
85.2.3	CONFIGURE PORT IPV6 SOURCE GUARD TO FILTER PACKET TYPE .....	1841
85.2.4	CONFIGURING STATIC BINDING ENTRIES FOR PORT IPV6 SOURCE GUARD.....	1842
85.2.5	CONFIGURE THE FUNCTION OF BINDING STATIC ENTRIES OF PORT MAC.....	1843
85.2.6	CONFIGURE GLOBAL IPV6 SOURCE GUARD FUNCTION.....	1844
85.2.7	IPV6 SOURCE GUARD MONITORING AND MAINTAINING .....	1845
<b>85.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF IPV6 SOURCE GUARD</b> .....	<b>1845</b>
85.3.1	CONFIGURE VALID PORT IPV6 SOURCE GUARD FUNCTION BASED ON DYNAMIC ENTRIES OF DHCPV6 SNOOPING.....	1845
85.3.2	CONFIGURE THE PORT IPV6 SOURCE GUARD FUNCTION WHICH TAKES EFFECT BASED ON STATIC ENTRIES.....	1848
<b>86</b>	<b>ND SNOOPING</b> .....	<b>1851</b>
<b>86.1</b>	<b>OVERVIEW</b> .....	<b>1851</b>
<b>86.2</b>	<b>ND SNOOPING FUNCTION CONFIGURATION</b> .....	<b>1851</b>
86.2.1	CONFIGURE ENABLING THE ND SNOOPING FUNCTION .....	1852
86.2.2	CONFIGURE SPECIFYING TRUSTED INTERFACE OF ND SNOOPING .....	1853
86.2.3	CONFIGURE STATIC BINDING ENTRIES FOR ND SNOOPING .....	1853
<b>86.2.4</b>	<b>CONFIGURE DYNAMIC BINDING TABLE DETECTION FUNCTION FOR ND SNOOPING</b> .....	<b>1854</b>
<b>86.2.5</b>	<b>CONFIGURE ENABLING ND SNOOPING ATTACK DETECTION LOG FUNCTION</b> .....	<b>1855</b>
<b>86.2.6</b>	<b>ND MONITORING AND MAINTAINING</b> .....	<b>1855</b>
<b>86.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF ND SNOOPING</b> .....	<b>1856</b>
<b>86.3.1</b>	<b>CONFIGURE THE BASIC FUNCTIONS OF ND SNOOPING</b> .....	<b>1856</b>
<b>87</b>	<b>DHCP SNOOPING</b> .....	<b>1859</b>
<b>87.1</b>	<b>OVERVIEW</b> .....	<b>1859</b>
87.1.1	BASIC FUNCTIONS OF DHCP SNOOPING .....	1859
87.1.2	DHCP SNOOPING OPTION82 .....	1859
<b>87.2</b>	<b>DHCP SNOOPING FUNCTION CONFIGURATION</b> .....	<b>1860</b>
87.2.1	CONFIGURE BASIC FUNCTIONS OF DHCP SNOOPING .....	1861

87.2.2	CONFIGURE DHCP SNOOPING OPTION82 .....	1864
87.2.3	CONFIGURE BINDING ENTRIES STORAGE FOR ND SNOOPING .....	1868
87.2.4	DHCP SNOOPING MONITORING AND MAINTAINING.....	1870
<b>87.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF DHCP SNOOPING.....</b>	<b>1871</b>
87.3.1	CONFIGURE BASIC FUNCTIONS OF DHCP SNOOPING .....	1871
<b>88</b>	<b>DHCPV6 SNOOPING .....</b>	<b>1873</b>
<b>88.1</b>	<b>OVERVIEW.....</b>	<b>1873</b>
88.1.1	BASIC FUNCTIONS OF DHCPV6 SNOOPING.....	1873
88.1.2	DHCPV6 SNOOPING OPTION18/37.....	1873
<b>88.2</b>	<b>DHCPV6 SNOOPING FUNCTION CONFIGURATION .....</b>	<b>1874</b>
88.2.1	CONFIGURE BASIC FUNCTIONS OF DHCPV6 SNOOPING.....	1875
88.2.2	CONFIGURE DHCPV6 SNOOPING OPTION18/37.....	1877
88.2.3	CONFIGURE DELAY TIME OF DELETING INVALID ENTRIES OF DHCPV6 SNOOPING .....	1881
88.2.4	CONFIGURE STORAGE OF BINDING ENTRIES OF DHCPV6 SNOOPING .....	1882
88.2.5	DHCPV6 SNOOPING MONITORING AND MAINTAINING .....	1883
<b>88.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF DHCPV6 SNOOPING .....</b>	<b>1884</b>
88.3.1	CONFIGURE BASIC FUNCTIONS OF DHCPV6 SNOOPING.....	1884
<b>89</b>	<b>DYNAMIC ARP INSPECTION .....</b>	<b>1886</b>
<b>89.1</b>	<b>OVERVIEW.....</b>	<b>1886</b>
<b>89.2</b>	<b>DYNAMIC ARP INSPECTION FUNCTION CONFIGURATION .....</b>	<b>1887</b>
89.2.1	CONFIGURE DYNAMIC ARP INSPECTION FUNCTION OF PORT.....	1887
89.2.2	CONFIGURE GLOBAL DYNAMIC ARP INSPECTION FUNCTION.....	1890
89.2.3	CONFIGURE DYNAMIC ARP INSPECTION TO DETECT ARP ATTACK .....	1890
89.2.4	DYNAMIC ARP INSPECTION MONITORING AND MAINTAINING .....	1891
<b>89.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF DAI .....</b>	<b>1892</b>
89.3.1	CONFIGURE BASIC FUNCTIONS OF DAI .....	1892
89.3.2	COMBINATION OF DAI WITH DHCP SNOOPING .....	1894
<b>90</b>	<b>HOST GUARD.....</b>	<b>1897</b>
<b>90.1</b>	<b>OVERVIEW.....</b>	<b>1897</b>
<b>90.2</b>	<b>HOST GUARD FUNCTION CONFIGURATION.....</b>	<b>1898</b>
90.2.1	CONFIGURE HOST GUARD FUNCTION .....	1898
90.2.2	HOST GUARD MONITORING AND MAINTAINING .....	1900
<b>91</b>	<b>AAA .....</b>	<b>1901</b>

<b>91.1</b>	<b>OVERVIEW.....</b>	<b>1901</b>
<b>91.2</b>	<b>AAA FUNCTION CONFIGURATION.....</b>	<b>1902</b>
91.2.1	CONFIGURE AAA DOMAIN .....	1903
91.2.2	CONFIGURE AUTHENTICATION FUNCTION UNDER AAA DOMAIN.....	1904
91.2.3	CONFIGURE AUTHORIZATION FUNCTION UNDER AAA DOMAIN .....	1905
91.2.4	CONFIGURE ACCOUNTING FUNCTION UNDER AAA DOMAIN.....	1907
91.2.5	CONFIGURE THE AUTHENTICATION METHOD OF ENTERING PRIVILEGED MODE .....	1908
91.2.6	CONFIGURE TO ENABLE COMMAND LINE AUTHORIZATION .....	1909
91.2.7	CONFIGURE THE SYSTEM EVENT ACCOUNTING FUNCTION.....	1910
91.2.8	CONFIGURE STATISTICS-RELATED PROPERTIES.....	1911
91.2.9	CONFIGURE RADIUS PROGRAM.....	1912
91.2.10	CONFIGURE TACACS PROGRAM.....	1916
91.2.11	AAA MONITORING AND MAINTAINING .....	1918
<b>91.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF AAA.....</b>	<b>1918</b>
91.3.1	CONFIGURE TELNET USER LOGIN FOR LOCAL AUTHENTICATION .....	1918
91.3.2	CONFIGURE TELNET USER LOGIN FOR RADIUS AUTHENTICATION, AUTHORIZATION AND ACCOUNTING .....	1919
91.3.3	CONFIGURE TELNET USER LEVEL SWITCH FOR RADIUS AUTHENTICATION.....	1921
91.3.4	CONFIGURE TACACS AUTHORIZATION AND ACCOUNTING OF SHELL COMMAND .....	1923
<b>92</b>	<b>802.1X.....</b>	<b>1926</b>
<b>92.1</b>	<b>OVERVIEW.....</b>	<b>1926</b>
92.1.1	802.1X.....	1926
92.1.2	SECURE CHANNEL AUTHENTICATION .....	1930
92.1.3	MAC ADDRESS AUTHENTICATION .....	1930
<b>92.2</b>	<b>802.1X FUNCTION CONFIGURATION.....</b>	<b>1931</b>
92.2.1	CONFIGURE 802.1X AUTHENTICATION FUNCTION .....	1933
92.2.2	CONFIGURE SECURE CHANNEL AUTHENTICATION.....	1935
92.2.3	CONFIGURE 802.1X AUTHENTICATION AND SECURE CHANNEL AUTHENTICATION ATTRIBUTES.....	1939
92.2.4	CONFIGURE MAC ADDRESS AUTHENTICATION.....	1946
92.2.5	CONFIGURE COMMON ATTRIBUTES.....	1953
92.2.6	802.1X MONITORING AND MAINTAINING .....	1974
<b>92.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF 802.1X FUNCTION .....</b>	<b>1976</b>
92.3.1	CONFIGURE PORTBASED AUTHENTICATION OF 802.1X.....	1976

92.3.2	CONFIGURE MACBASED AUTHENTICATION OF 802.1X.....	1978
92.3.3	CONFIGURE TRANSPARENT TRANSMISSION MODE OF 802.1X.....	1980
92.3.4	CONFIGURE 802.1X FREE-CLIENT AUTHENTICATION.....	1983
92.3.5	CONFIGURE SECURE CHANNEL .....	1985
92.3.6	CONFIGURE IP AUTHORIZATION AS DHCP SERVER MODE .....	1987
92.3.7	CONFIGURE 802.1X CRITICAL VLAN .....	1990
92.3.8	CONFIGURE COMBINED USE OF 802.1X AND PORT SECURITY.....	1992
<b>93</b>	<b>PORTAL .....</b>	<b>1995</b>
93.1	OVERVIEW.....	1995
93.1.1	INTRODUCTION .....	1995
93.1.2	SYSTEM COMPOSITION OF PORTAL.....	1995
93.1.3	AUTHENTICATION METHOD OF PORTAL.....	1996
93.1.4	AUTHENTICATION PROCESS OF PORTAL.....	1997
93.1.5	SUPPORT ISSUING ACL .....	1999
93.2	PORTAL FUNCTION CONFIGURATION .....	1999
93.2.1	CONFIGURE PORTAL SERVER AND ATTRIBUTES .....	2000
93.2.2	CONFIGURE LAYER-2 PORTAL AUTHENTICATION FUNCTION .....	2003
93.2.3	CONFIGURE LAYER-2 PORTAL AUTHENTICATION ATTRIBUTES .....	2005
93.2.4	CONFIGURE LAYER-3 PORTAL AUTHENTICATION FUNCTION .....	2006
93.2.5	CONFIGURE COMMON ATTRIBUTES.....	2008
93.2.6	PORTAL MONITORING AND MAINTAINING.....	2013
93.3	TYPICAL CONFIGURATION EXAMPLE OF PORTAL.....	2015
93.3.1	CONFIGURE PORTBASED LAYER-2 PORTAL AUTHENTICATION.....	2015
93.3.2	CONFIGURE MACBASED LAYER-2 PORTAL AUTHENTICATION .....	2017
93.3.3	CONFIGURE GENERAL LAYER-3 PORTAL AUTHENTICATION .....	2019
<b>94</b>	<b>TRUSTED DEVICE ACCESS .....</b>	<b>2022</b>
94.1	OVERVIEW.....	2023
94.2	CONFIGURATION OF TRUSTED DEVICE ACCESS.....	2023
94.2.1	CONFIGURE TRUSTED DEVICE ACCESS.....	2024
94.2.2	CONFIGURE 802.1X DEVICE AUTHENTICATION.....	2028
94.2.3	TRUSTED DEVICE ACCESS MONITORING AND MAINTAINING .....	2030
94.3	TYPICAL CONFIGURATION EXAMPLE OF TRUSTED DEVICE ACCESS .....	2031
<b>95</b>	<b>ACL CONFIGURATION .....</b>	<b>2034</b>

<b>95.1 OVERVIEW.....</b>	<b>2034</b>
95.1.1 OVERVIEW .....	2034
95.1.2 TIME DOMAIN .....	2035
<b>95.2 ACL FUNCTION CONFIGURATION .....</b>	<b>2035</b>
95.2.1 CONFIGURE STANDARD IP ACL.....	2037
95.2.2 CONFIGURE EXTENDED IP ACL.....	2039
95.2.3 CONFIGURE STANDARD MAC ACL .....	2043
95.2.4 CONFIGURE EXTENDED MAC ACL .....	2045
95.2.5 CONFIGURE EXTENDED HYBRID ACL .....	2048
95.2.6 CONFIGURE STANDARD IPV6 ACL .....	2051
95.2.7 CONFIGURE EXTENDED IPV6 ACL .....	2054
95.2.8 CONFIGURE COMMIT OPERATION .....	2056
95.2.9 CONFIGURE LIMIT OF ACL RULE ENTRIES .....	2057
95.2.10 CONFIGURE TIME DOMAIN.....	2058
95.2.11 CONFIGURE ACL APPLICATION .....	2062
95.2.12 CONFIGURE ACL MODE .....	2075
95.2.13 ACL MONITORING AND MAINTAINING .....	2075
<b>95.3 TYPICAL CONFIGURATION EXAMPLE OF ACL .....</b>	<b>2076</b>
95.3.1 CONFIGURE STANDARD IP ACL.....	2076
95.3.2 CONFIGURE EXTENDED IP ACL WITH TIME DOMAIN .....	2078
95.3.3 CONFIGURE STANDARD MAC ACL .....	2080
95.3.4 CONFIGURE EXTENDED MAC ACL .....	2082
95.3.5 CONFIGURE EXTENDED HYBRID ACL .....	2084
<b>96 ATTACK DETECTION.....</b>	<b>2087</b>
<b>96.1 OVERVIEW.....</b>	<b>2087</b>
<b>96.2 ATTACK DEFENSE FUNCTION CONFIGURATION.....</b>	<b>2087</b>
96.2.1 CONFIGURE SINGLE-PACKET ATTACK DEFENSE FUNCTION .....	2088
96.2.2 CONFIGURE FLOOD DEFENSE FUNCTION .....	2089
96.2.3 CONFIGURE SCANNING ATTACK DEFENSE FUNCTION.....	2093
96.2.4 CONFIGURE URPF ATTACK DEFENSE FUNCTION .....	2096
96.2.5 CONFIGURE BLACKLIST FUNCTION.....	2097
96.2.6 ATTACK DEFENSE MONITORING AND MAINTAINING .....	2098
<b>96.3 TYPICAL CONFIGURATION EXAMPLE OF ATTACK DEFENSE.....</b>	<b>2100</b>

96.3.1	CONFIGURE SINGLE-PACKET ATTACK DETECTION .....	2100
96.3.2	CONFIGURE FLOOD ATTACK DETECTION .....	2102
96.3.3	CONFIGURE SCANNING ATTACK DETECTION .....	2104
96.3.4	CONFIGURE URPF STRICT MODE .....	2107
96.3.5	CONFIGURE URPF LOOSE MODE .....	2108
<b>97</b>	<b>AARF .....</b>	<b>2112</b>
<b>97.1</b>	<b>OVERVIEW .....</b>	<b>2112</b>
<b>97.2</b>	<b>INTRODUCTION .....</b>	<b>2112</b>
<b>97.3</b>	<b>PRINCIPLE .....</b>	<b>2112</b>
<b>97.4</b>	<b>ARP-GUARD .....</b>	<b>2113</b>
<b>97.4.1</b>	<b>ARP-GUARD FUNCTION CONFIGURATION .....</b>	<b>2113</b>
<b>97.4.2</b>	<b>CONFIGURE BASIC FUNCTIONS OF ARP-GUARD .....</b>	<b>2114</b>
<b>97.4.3</b>	<b>CONFIGURE ARP-GUARD MONITORING POLICY .....</b>	<b>2115</b>
<b>97.4.4</b>	<b>ARP-GUARD MONITORING AND MAINTAINING .....</b>	<b>2117</b>
<b>97.5</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF AARF ARP-GUARD .....</b>	<b>2117</b>
<b>97.5.1</b>	<b>CONFIGURE BASIC FUNCTIONS OF AARF ARP-GUARD .....</b>	<b>2117</b>
<b>98</b>	<b>PPPOE+ .....</b>	<b>2121</b>
<b>98.1</b>	<b>INTRODUCTION TO BASIC FUNCTIONS OF PPPOE+ .....</b>	<b>2121</b>
<b>98.2</b>	<b>PRINCIPLE .....</b>	<b>2121</b>
<b>98.3</b>	<b>VENDOR-SPECIFIC TAG FOR PPPOE PACKET .....</b>	<b>2122</b>
<b>98.4</b>	<b>CONFIGURE BASIC FUNCTIONS OF PPPOE+ .....</b>	<b>2123</b>
<b>98.4.1</b>	<b>CONFIGURE TO ENABLE/DISABLE PPPOE+ FUNCTION .....</b>	<b>2123</b>
<b>98.4.2</b>	<b>CONFIGURE PROCESSING POLICY OF PPPOE+ FUNCTION FOR PPPOE PACKET WITH VENDOR-SPECIFIC TAG .....</b>	<b>2124</b>
<b>98.4.3</b>	<b>CONFIGURE CONTENT OF CIRCUIT-ID IN VENDOR-SPECIFIC TAG .....</b>	<b>2125</b>
<b>98.4.4</b>	<b>CONFIGURE CONTENT OF REMOTE-ID IN VENDOR-SPECIFIC TAG .....</b>	<b>2126</b>
<b>98.4.5</b>	<b>CONFIGURE FILL POLICY OF PPPOE+ FUNCTION FOR VENDOR-SPECIFIC TAG CONTAINED IN PPPOE PACKET .....</b>	<b>2127</b>
<b>98.4.6</b>	<b>CONFIGURE TO FILL VALUE OF VENDOR-ID IN VENDOR-SPECIFIC TAG .....</b>	<b>2128</b>
<b>99</b>	<b>HA .....</b>	<b>2129</b>
<b>99.1</b>	<b>OVERVIEW .....</b>	<b>2129</b>
<b>99.2</b>	<b>HA FUNCTION CONFIGURATION .....</b>	<b>2129</b>
<b>99.2.1</b>	<b>HA MONITORING AND MAINTAINING .....</b>	<b>2129</b>

<b>100</b>	<b>ULFD</b>	<b>2130</b>
<b>100.1</b>	<b>OVERVIEW</b>	<b>2130</b>
<b>100.2</b>	<b>ULFD FUNCTION CONFIGURATION</b>	<b>2131</b>
100.2.1	CONFIGURE ULFD BASIC FUNCTIONS	2131
100.2.2	CONFIGURE ULFD PARAMETERS	2133
100.2.3	ULFD MONITORING AND MAINTAINING	2134
<b>100.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF ULFD</b>	<b>2134</b>
100.3.1	CONFIGURE ULFD BASIC FUNCTIONS	2134
<b>101</b>	<b>EIPS</b>	<b>2137</b>
<b>101.1</b>	<b>OVERVIEW</b>	<b>2137</b>
101.1.1	BASIC CONCEPTS	2137
101.1.2	OPERATING MECHANISM	2139
101.1.3	TYPICAL TOPOLOGY OF SUBRING MODE	2140
101.1.4	TYPICAL TOPOLOGY OF HIERARCHY SEGMENT MODE	2141
<b>101.2</b>	<b>EIPS FUNCTION CONFIGURATION</b>	<b>2142</b>
101.2.1	CONFIGURE EIPS RING	2143
101.2.2	CONFIGURE EIPS RELIABILITY	2152
101.2.3	CONFIGURE EIPS TIMER	2153
101.2.4	EIPS MONITORING AND MAINTAINING	2154
<b>101.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF EIPS</b>	<b>2155</b>
101.3.1	CONFIGURE SINGLE RING IN EIPS HIERARCHY SEGMENT MODE	2155
101.3.2	CONFIGURE THE INTERSECTING RINGS IN EIPS HIERARCHY SEGMENT MODE	2163
101.3.3	CONFIGURE THE INTERSECTING RINGS IN EIPS SUBRING MODE	2178
<b>102</b>	<b>ULPP AND MONITOR LINK</b>	<b>2196</b>
<b>102.1</b>	<b>OVERVIEW</b>	<b>2196</b>
<b>102.2</b>	<b>ULPP FUNCTION CONFIGURATION</b>	<b>2196</b>
102.2.1	CONFIGURE BASIC FUNCTIONS OF ULPP	2197
102.2.2	CONFIGURE ULPP COMPATIBLE MODE	2200
102.2.3	CONFIGURE BASIC FUNCTIONS OF MONITOR LINK GROUP	2201
102.2.4	ULPP MONITORING AND MAINTAINING	2202
<b>102.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF ULPP AND MONITOR LINK</b>	<b>2203</b>
102.3.1	CONFIGURE ULPP	2203
102.3.2	CONFIGURE MONITOR LINK	2206

<b>103</b>	<b>VRRP</b> .....	<b>2210</b>
<b>103.1</b>	<b>OVERVIEW</b> .....	<b>2210</b>
<b>103.2</b>	<b>VRRP FUNCTION CONFIGURATION</b> .....	<b>2210</b>
103.2.1	CONFIGURE BASIC FUNCTIONS OF VRRP .....	2211
103.2.2	CONFIGURE VRRP COORDINATION GROUP.....	2214
103.2.3	CONFIGURE VRRP NETWORK AUTHENTICATION.....	2215
103.2.4	CONFIGURE VRRP DELAY DOWNGRADING.....	2216
103.2.5	CONFIGURE VRRP PACKET DISPERSION .....	2217
103.2.6	CONFIGURE VRRP DELAYED RECOVERY .....	2217
103.2.7	CONFIGURE VIRTUAL MAC ADDRESS OF VRRP DUAL-HOLDING.....	2218
103.2.8	CONFIGURE STATIC VRRP FUNCTION.....	2219
103.2.9	CONFIGURE COORDINATION OF VRRP WITH TRACK.....	2219
103.2.10	VRRP MONITORING AND MAINTAINING.....	2223
<b>103.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF VRRP</b> .....	<b>2223</b>
103.3.1	CONFIGURE THE PRIORITY OF SINGLE VRRP BACKUP GROUP .....	2223
103.3.2	CONFIGURE VRRP COORDINATION GROUP.....	2225
103.3.3	CONFIGURE COORDINATION OF VRRP WITH TRACK.....	2230
103.3.4	CONFIGURE COORDINATION OF VRRP WITH BFD.....	2232
103.3.5	CONFIGURE VRRP LOAD BALANCING .....	2236
<b>104</b>	<b>VRRPV3</b> .....	<b>2239</b>
<b>104.1</b>	<b>OVERVIEW</b> .....	<b>2239</b>
<b>104.2</b>	<b>VRRPV3 FUNCTION CONFIGURATION</b> .....	<b>2239</b>
104.2.1	CONFIGURE BASIC FUNCTIONS OF VRRPV3.....	2240
104.2.2	CONFIGURE STATIC VRRPV3 FUNCTIONS .....	2242
104.2.3	CONFIGURE COORDINATION OF VRRPV3 WITH TRACK .....	2243
104.2.4	VRRPV3 MONITORING AND MAINTAINING .....	2246
<b>104.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF VRRPV3</b> .....	<b>2247</b>
104.3.1	CONFIGURE IPV6-BASED SINGLE VRRP BACKUP GROUP.....	2247
104.3.2	CONFIGURE IPV6-BASED COORDINATION OF VRRP WITH TRACK.....	2249
104.3.3	CONFIGURE IPV6-BASED VRRP LOAD BALANCING .....	2252
<b>105</b>	<b>VBRP</b> .....	<b>2258</b>
<b>105.1</b>	<b>OVERVIEW</b> .....	<b>2258</b>
<b>105.2</b>	<b>VBRP FUNCTION CONFIGURATION</b> .....	<b>2258</b>

105.2.1	CONFIGURE BASIC FUNCTIONS OF VBRP .....	2259
105.2.2	CONFIGURE VBRP NETWORK AUTHENTICATION .....	2261
105.2.3	CONFIGURE COORDINATION OF VBRP WITH TRACK .....	2263
105.2.4	VBRP MONITORING AND MAINTAINING .....	2265
<b>105.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF VBRP .....</b>	<b>2265</b>
105.3.1	CONFIGURE BASIC MODE OF VBRP .....	2265
105.3.2	CONFIGURE COORDINATION OF VBRP WITH TRACK .....	2267
105.3.3	CONFIGURE VBRP LOAD BALANCING MODE .....	2270
<b>106</b>	<b>LOAD-BALANCE VIRTUAL ROUTER REDUNDANCY PROTOCOL .....</b>	<b>2273</b>
<b>106.1</b>	<b>OVERVIEW .....</b>	<b>2273</b>
<b>106.2</b>	<b>LOAD-BALANCE VIRTUAL ROUTER REDUNDANCY PROTOCOL FUNCTION CONFIGURATION 2273</b>	
106.2.1	CONFIGURE CURRENT MODE OF LOAD-BALANCE VRRP .....	2274
106.2.2	CONFIGURE BASIC FUNCTIONS OF LOAD-BALANCE VRRP .....	2274
106.2.3	CONFIGURE TIMER OF LOAD-BALANCE VRRP .....	2277
106.2.4	LOAD-BALANCE VRRP MONITORING AND MAINTAINING .....	2280
<b>106.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF LOAD-BALANCE VRRP .....</b>	<b>2281</b>
106.3.1	CONFIGURE BASIC FUNCTIONS OF LOAD-BALANCE VRRP .....	2281
<b>107</b>	<b>TRACK .....</b>	<b>2285</b>
<b>107.1</b>	<b>OVERVIEW .....</b>	<b>2285</b>
<b>107.2</b>	<b>TRACK FUNCTION CONFIGURATION .....</b>	<b>2285</b>
107.2.1	CONFIGURE TRACK GROUP .....	2286
107.2.2	CONFIGURE MONITORING OBJECT .....	2287
107.2.3	TRACK MONITORING AND MAINTAINING .....	2293
<b>108</b>	<b>BFD .....</b>	<b>2294</b>
<b>108.1</b>	<b>OVERVIEW .....</b>	<b>2294</b>
<b>108.2</b>	<b>BFD FUNCTION CONFIGURATION .....</b>	<b>2295</b>
108.2.1	CONFIGURE BASIC FUNCTIONS OF BFD .....	2295
108.2.2	BFD MONITORING AND MAINTAINING .....	2302
<b>108.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF BFD .....</b>	<b>2302</b>
108.3.1	CONFIGURE BASIC FUNCTIONS OF BFD .....	2302
<b>109</b>	<b>EEP .....</b>	<b>2306</b>
<b>109.1</b>	<b>OVERVIEW .....</b>	<b>2306</b>

<b>109.2</b>	<b>EEP FUNCTION CONFIGURATION.....</b>	<b>2306</b>
109.2.1	CONFIGURE EEP POLICY.....	2306
109.2.2	CONFIGURE EEP EVENT.....	2307
109.2.3	CONFIGURE EEP ACTION.....	2310
109.2.4	EEP MONITORING AND MAINTAINING .....	2310
<b>109.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF EEP.....</b>	<b>2311</b>
109.3.1	CONFIGURE EEP POLICY AND PBR COORDINATION .....	2311
<b>110</b>	<b>ERPS .....</b>	<b>2315</b>
<b>110.1</b>	<b>OVERVIEW.....</b>	<b>2315</b>
<b>110.2</b>	<b>ERPS FUNCTION CONFIGURATION .....</b>	<b>2316</b>
110.2.1	CONFIGURE ERPS RING .....	2317
110.2.2	CONFIGURE ERPS RING TIMER .....	2320
110.2.3	CONFIGURE ERPS NETWORK OPTIMIZATION .....	2321
110.2.4	CONFIGURE COORDINATION OF ERPS WITH CFM.....	2323
110.2.5	ERPS MONITORING AND MAINTAINING.....	2325
<b>110.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF ERPS .....</b>	<b>2325</b>
110.3.1	CONFIGURE BASIC FUNCTIONS OF ERPS.....	2325
110.3.2	CONFIGURE ERPS LOAD.....	2330
110.3.3	CONFIGURE ERPS INTERSECTING RINGS.....	2337
<b>111</b>	<b>NETWORK TEST AND FAULT DIAGNOSIS .....</b>	<b>2345</b>
<b>111.1</b>	<b>OVERVIEW.....</b>	<b>2345</b>
<b>111.2</b>	<b>NETWORK TEST AND FAULT DIAGNOSIS APPLICATION .....</b>	<b>2345</b>
111.2.1	PING FUNCTION .....	2346
111.2.2	TRACEROUTE FUNCTION.....	2351
111.2.3	SYSTEM DEBUGGING FUNCTION .....	2354
111.2.4	NETWORK TEST AND FAULT DIAGNOSIS MONITORING AND MAINTAINING .....	2355
<b>111.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF NETWORK TEST AND FAULT DIAGNOSIS.....</b>	<b>2355</b>
111.3.1	APPLICATION OF PING .....	2355
111.3.2	APPLICATION OF TRACEROUTE .....	2357
<b>112</b>	<b>KEEPALIVE GATEWAY .....</b>	<b>2359</b>
<b>112.1</b>	<b>OVERVIEW.....</b>	<b>2359</b>
<b>112.2</b>	<b>KEEPALIVE GATEWAY FUNCTION CONFIGURATION .....</b>	<b>2359</b>
112.2.1	CONFIGURE KEEPALIVE GATEWAY.....	2359

112.2.2	KEEPALIVE GATEWAY MONITORING AND MAINTAINING .....	2361
<b>112.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF KEEPALIVE GATEWAY .....</b>	<b>2361</b>
112.3.1	CONFIGURE KEEPALIVE GATEWAY FUNCTION. ....	2361
<b>113</b>	<b>SLA .....</b>	<b>2365</b>
<b>113.1</b>	<b>OVERVIEW.....</b>	<b>2365</b>
<b>113.2</b>	<b>SLA FUNCTION CONFIGURATION.....</b>	<b>2365</b>
113.2.1	ENABLE RTR. ....	2366
113.2.2	CONFIGURE AN RTR ENTITY. ....	2367
113.2.3	CONFIGURE RTR ENTITY GROUP.....	2381
113.2.4	CONFIGURE RTR RESPONDER.....	2383
113.2.5	CONFIGURE RTR SCHEDULER.....	2384
113.2.6	CONFIGURE PAUSING SCHEDULING ENTITY .....	2384
113.2.7	CONFIGURE RESTORING SCHEDULING ENTITY .....	2385
113.2.8	SLA MONITORING AND MAINTAINING.....	2386
<b>113.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF SLA.....</b>	<b>2386</b>
113.3.1	CONFIGURE AN ICMP-ECHO ENTITY TO DETECT THE NETWORK COMMUNICATION.....	2386
113.3.2	CONFIGURE AN ICMP-PATH-ECHO ENTITY TO DETECT THE NETWORK COMMUNICATION ....	2389
113.3.3	CONFIGURE AN ICMP-PATH-JITTER ENTITY TO DETECT THE NETWORK COMMUNICATION ...	2392
113.3.4	CONFIGURING A VOIP-JITTER ENTITY TO DETECT NETWORK TRANSMISSION OF VOICE PACKETS	2394
113.3.5	CONFIGURING A UDP-ECHO ENTITY TO DETECT NETWORK TRANSMISSION OF UDP PACKETS 2397	
113.3.6	CONFIGURE THE FLOW-STATISTICS ENTITY TO DETECT INTERFACE TRAFFIC FLOW .....	2399
<b>113.3.7</b>	<b>CONFIGURING AN ICMP-ECHO IPV6 ENTITY TO DETECT NETWORK COMMUNICATION</b>	<b>2402</b>
113.3.8	CONFIGURE TRACK TO COORDINATE WITH SLA .....	2405
<b>113.3.9</b>	<b>CONFIGURE TRACK TO COORDINATE WITH ICMP-ECHO IPV6 .....</b>	<b>2407</b>
<b>114</b>	<b>NTP .....</b>	<b>2409</b>
<b>114.1</b>	<b>OVERVIEW.....</b>	<b>2409</b>
<b>114.2</b>	<b>NTP FUNCTION CONFIGURATION.....</b>	<b>2410</b>
<b>114.2.1</b>	<b>CONFIGURE NTP BASIC FUNCTIONS.....</b>	<b>2411</b>
<b>114.2.2</b>	<b>CONFIGURE NTP OPTIONAL PARAMETERS.....</b>	<b>2414</b>
<b>114.2.3</b>	<b>CONFIGURE THE NTP AUTHENTICATION FUNCTION.....</b>	<b>2417</b>
<b>114.2.4</b>	<b>CONFIGURE THE NTP ACCESS CONTROL.....</b>	<b>2421</b>
<b>114.2.5</b>	<b>NTP MONITORING AND MAINTAINING .....</b>	<b>2422</b>

<b>114.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF NTP.....</b>	<b>2422</b>
114.3.1	CONFIGURE THE NTP IPV4 SERVER AND CLIENT .....	2422
114.3.2	CONFIGURE THE NTP IPV4 SERVER AND MULTI-LEVEL CLIENT .....	2424
114.3.3	CONFIGURE NTP SERVER AND CLIENT WITH MD5 AUTHENTICATION.....	2425
114.3.4	CONFIGURE THE NTP IPV4 P2P MODE.....	2427
114.3.5	CONFIGURE NTP BROADCAST MODE .....	2429
114.3.6	CONFIGURE THE NTP IPV6 SERVER AND CLIENT .....	2431
114.3.7	CONFIGURE THE NTP IPV6 P2P MODE.....	2433
<b>115</b>	<b>PORT MIRROR .....</b>	<b>2435</b>
<b>115.1</b>	<b>OVERVIEW.....</b>	<b>2435</b>
115.1.1	OVERVIEW .....	2435
115.1.2	BASIC CONCEPTS.....	2435
<b>115.2</b>	<b>SPAN FUNCTION CONFIGURATION .....</b>	<b>2437</b>
115.2.1	CONFIGURE LOCAL SPAN.....	2437
115.2.2	CONFIGURE RSPAN .....	2438
115.2.3	CONFIGURE ERSPAN.....	2441
115.2.4	CONFIGURE VLAN SPAN.....	2442
115.2.5	SPAN MONITORING AND MAINTAINING .....	2443
<b>115.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF PORT MIRRORING.....</b>	<b>2445</b>
115.3.1	CONFIGURE LOCAL SPAN.....	2445
115.3.2	CONFIGURE RSPAN .....	2446
115.3.3	CONFIGURE ERSPAN.....	2448
115.3.4	CONFIGURE VLAN SPAN.....	2450
<b>116</b>	<b>LLDP .....</b>	<b>2452</b>
<b>116.1</b>	<b>OVERVIEW.....</b>	<b>2452</b>
116.1.1	OVERVIEW OF LLDP PROTOCOL .....	2452
116.1.2	TLV TYPE INFORMATION .....	2452
116.1.3	LLDP WORKING MECHANISM .....	2457
<b>116.2</b>	<b>LLDP FUNCTION CONFIGURATION.....</b>	<b>2458</b>
116.2.1	CONFIGURE LLDP BASIC FUNCTIONS. ....	2459
116.2.2	CONFIGURE THE LLDP WORKING MODE.....	2460
116.2.3	CONFIGURE TLV ALLOWED TO BE RELEASED BY LLDP .....	2462
116.2.4	CONFIGURE LLDP PARAMETERS.....	2464

116.2.5	LLDP MONITORING AND MAINTAINING .....	2467
<b>116.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF LLDP .....</b>	<b>2469</b>
116.3.1	CONFIGURE THE BASIC FUNCTIONS OF LLDP .....	2469
<b>117</b>	<b>SNMP .....</b>	<b>2471</b>
<b>117.1</b>	<b>OVERVIEW .....</b>	<b>2471</b>
<b>117.2</b>	<b>SNMP FUNCTION CONFIGURATION .....</b>	<b>2474</b>
117.2.1	CONFIGURE BASIC FUNCTIONS OF SNMP .....	2475
117.2.2	CONFIGURE SNMPv1/v2 .....	2477
117.2.3	CONFIGURE SNMPv3. ....	2478
117.2.4	CONFIGURE SNMP TRAP .....	2482
117.2.5	SNMP MONITORING AND MAINTAINING .....	2483
<b>117.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF SNMP .....</b>	<b>2484</b>
117.3.1	CONFIGURE AN SNMP v1/v2c PROXY SERVER .....	2484
117.3.2	CONFIGURE AN SNMP v3 PROXY SERVER .....	2486
117.3.3	CONFIGURE SNMP v3 TRAP ADVERTISEMENTS .....	2487
117.3.4	CONFIGURE SNMP v3 INFORM ADVERTISEMENTS .....	2489
117.3.5	CONFIGURE SNMP v3 AGENT FORWARDING .....	2491
<b>117.4</b>	<b>OVERVIEW .....</b>	<b>2494</b>
<b>117.5</b>	<b>RMON FUNCTION CONFIGURATION .....</b>	<b>2495</b>
117.5.1	ENABLE THE RMON FUNCTION .....	2495
117.5.2	CONFIGURE RMON ALARM GROUPS .....	2496
117.5.3	CONFIGURING RMON EXTENDED ALARM GROUPS .....	2497
117.5.4	CONFIGURE RMON EVENT GROUPS .....	2498
117.5.5	CONFIGURE RMON HISTORY GROUPS .....	2499
117.5.6	CONFIGURE RMON STATISTICS GROUPS .....	2500
117.5.7	RMON MONITORING AND MAINTAINING .....	2500
<b>117.6</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF RMON .....</b>	<b>2501</b>
117.6.1	CONFIGURE BASIC FUNCTIONS OF RMON .....	2501
<b>117.7</b>	<b>OVERVIEW .....</b>	<b>2505</b>
<b>117.8</b>	<b>CWMP FUNCTION CONFIGURATION .....</b>	<b>2506</b>
<b>117.8.1</b>	<b>CONFIGURE BASIC FUNCTIONS OF CWMP .....</b>	<b>2507</b>
<b>117.8.2</b>	<b>CONFIGURE CWMP AUTHENTICATION AND ENCRYPTION FUNCTIONS .....</b>	<b>2515</b>
<b>117.8.3</b>	<b>CONFIGURE CWMP EXTENDED FUNCTIONS .....</b>	<b>2517</b>

<b>117.8.4</b>	<b>CWMP MONITORING AND MAINTAINING .....</b>	<b>2519</b>
<b>117.9</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF CWMP .....</b>	<b>2520</b>
<b>117.9.1</b>	<b>CONFIGURE THE AUTHENTICATION FUNCTION OF CWMP .....</b>	<b>2520</b>
<b>117.9.2</b>	<b>CONFIGURE CWMP TO SPECIFY THE SOURCE IP ADDRESS .....</b>	<b>2521</b>
<b>117.9.3</b>	<b>CONFIGURE CWMP LINK BACKUP.....</b>	<b>2523</b>
<b>118</b>	<b>NETCONF .....</b>	<b>2526</b>
<b>118.1</b>	<b>OVERVIEW.....</b>	<b>2526</b>
<b>118.2</b>	<b>NETCONF BASIC FUNCTION CONFIGURATION.....</b>	<b>2526</b>
<b>118.2.1</b>	<b>NETCONF SERVER FUNCTIONS CONFIGURATION.....</b>	<b>2527</b>
<b>118.2.2</b>	<b>CONFIGURING THE FUNCTIONS OF NETCONF CALL-HOME.....</b>	<b>2528</b>
<b>118.2.3</b>	<b>NETCONF MONITORING AND MAINTAINING.....</b>	<b>2529</b>
<b>118.3</b>	<b>NETCONF TYPICAL CONFIGURATION EXAMPLE .....</b>	<b>2529</b>
<b>118.3.1</b>	<b>CONFIGURE THE NETCONF SERVER .....</b>	<b>2529</b>
<b>119</b>	<b>TELEMETRY .....</b>	<b>2532</b>
<b>119.1</b>	<b>OVERVIEW.....</b>	<b>2532</b>
<b>119.2</b>	<b>TELEMETRY FUNCTION CONFIGURATION .....</b>	<b>2532</b>
<b>119.2.1</b>	<b>CONFIGURE TELEMETRY STATIC SUBSCRIPTIONS .....</b>	<b>2533</b>
<b>119.2.2</b>	<b>CONFIGURING TELEMETRY DYNAMIC SUBSCRIPTIONS .....</b>	<b>2535</b>
<b>119.2.3</b>	<b>TELEMETRY MONITORING AND MAINTAINING .....</b>	<b>2536</b>
<b>119.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF TELEMETRY .....</b>	<b>2537</b>
<b>119.3.1</b>	<b>CONFIGURE TELEMETRY STATIC SUBSCRIPTIONS .....</b>	<b>2537</b>
<b>119.3.2</b>	<b>CONFIGURING TELEMETRY DYNAMIC SUBSCRIPTIONS .....</b>	<b>2538</b>
<b>120</b>	<b>SFLOW .....</b>	<b>2540</b>
<b>120.1</b>	<b>OVERVIEW.....</b>	<b>2540</b>
<b>120.2</b>	<b>SFLOW FUNCTION CONFIGURATION .....</b>	<b>2541</b>
<b>120.2.1</b>	<b>CONFIGURE BASIC FUNCTIONS OF SFLOW.....</b>	<b>2541</b>
<b>120.2.2</b>	<b>CONFIGURE SFLOW SAMPLING MODE .....</b>	<b>2543</b>
<b>120.2.3</b>	<b>SFLOW MONITORING AND MAINTAINING.....</b>	<b>2544</b>
<b>120.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF SFLOW .....</b>	<b>2545</b>
<b>120.3.1</b>	<b>CONFIGURE BASIC FUNCTIONS OF SFLOW.....</b>	<b>2545</b>
<b>121</b>	<b>VST .....</b>	<b>2547</b>
<b>121.1</b>	<b>OVERVIEW.....</b>	<b>2547</b>
<b>121.1.1</b>	<b>BASIC CONCEPTS.....</b>	<b>2549</b>

<b>121.2</b>	<b>VST FUNCTION CONFIGURATION.....</b>	<b>2550</b>
121.2.1	CONFIGURE VIRTUAL SWITCH MEMBER DEVICE.....	2551
121.2.2	CONFIGURE VIRTUAL SWITCH LINK INTERFACE.....	2554
121.2.3	CONFIGURE DEVICE RUNNING MODE.....	2555
121.2.4	CONFIGURE THE MAXIMUM NUMBER OF DEVICES SUPPORTED BY THE STACK SYSTEM.....	2556
121.2.5	VST MONITORING AND MAINTAINING.....	2557
<b>121.3</b>	<b>VST TYPICAL CONFIGURATION EXAMPLE.....</b>	<b>2558</b>
121.3.1	CONFIGURE THE DEVICES TO FORM CHAIN STACK SYSTEM.....	2558
<b>122</b>	<b>MAD.....</b>	<b>2561</b>
<b>122.1</b>	<b>OVERVIEW.....</b>	<b>2561</b>
<b>122.2</b>	<b>MAD FUNCTION CONFIGURATION.....</b>	<b>2562</b>
122.2.1	CONFIGURE MAD LACP FUNCTION.....	2562
122.2.2	CONFIGURE MAD FAST-HELLO FUNCTION.....	2563
122.2.3	CONFIGURE RESERVED PORT.....	2565
122.2.4	CONFIGURE RESTORING MAD STATUS TO ACTIVE STATUS.....	2566
122.2.5	MAD MONITORING AND MAINTAINING.....	2567
<b>122.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF MAD.....</b>	<b>2568</b>
122.3.1	CONFIGURE MAD LACP FUNCTION.....	2568
122.3.2	CONFIGURE MAD FAST-HELLO FUNCTION.....	2570
<b>123</b>	<b>MVST.....</b>	<b>2573</b>
<b>123.1</b>	<b>OVERVIEW.....</b>	<b>2573</b>
<b>123.2</b>	<b>MVST FUNCTION CONFIGURATION.....</b>	<b>2575</b>
123.2.1	CONFIGURE MVST BASIC FUNCTIONS.....	2576
123.2.2	CONFIGURE MVST PARAMETERS.....	2579
123.2.3	CONFIGURE MVST FEATURES.....	2582
123.2.4	MVST MONITORING AND MAINTAINING.....	2588
<b>123.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF MVST.....</b>	<b>2590</b>
123.3.1	CONFIGURE AUTO UPGRADE INSPECTION.....	2590
123.3.2	CONFIGURE AUTO ISSUE OF COMMON TEMPLATE.....	2596
123.3.3	CONFIGURE AUTO ISSUE OF BINDING CONFIGURATION.....	2604
<b>124</b>	<b>VD.....</b>	<b>2612</b>
<b>124.1</b>	<b>OVERVIEW.....</b>	<b>2612</b>
<b>124.2</b>	<b>VD FUNCTION CONFIGURATION.....</b>	<b>2613</b>

<b>124.2.1</b>	<b>CONFIGURE VD</b> .....	<b>2613</b>
<b>124.2.2</b>	<b>LOG IN TO VD</b> .....	<b>2614</b>
<b>124.2.3</b>	<b>VD MONITORING AND MAINTAINING</b> .....	<b>2615</b>
<b>124.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF VD</b> .....	<b>2615</b>
<b>125</b>	<b>TRILL</b> .....	<b>2617</b>
<b>125.1</b>	<b>OVERVIEW</b> .....	<b>2617</b>
125.1.1	BASIC CONCEPTS.....	2618
125.1.2	TRILL FRAME FORMAT .....	2619
125.1.3	TRILL FORWARDING MECHANISM .....	2621
<b>125.2</b>	<b>TRILL FUNCTION CONFIGURATION</b> .....	<b>2625</b>
125.2.1	ENABLE THE TRILL PROTOCOL GLOBALLY .....	2627
125.2.2	CONFIGURE SYSTEM ID AND NICKNAME.....	2628
125.2.3	ENABLE THE TRILL PROTOCOL ON THE PORT .....	2630
125.2.4	CONFIGURE THE DRB PRIORITY OF THE PORT .....	2632
125.2.5	CONFIGURE ADVERTISING VLAN AND DESIGNATED VLAN OF THE PORT .....	2634
125.2.6	CONFIGURE VLAN FORWARDER .....	2637
125.2.7	CONFIGURE PSEUDO-NODE MODE OF THE PORT.....	2638
125.2.8	CONFIGURE LINK OVERHEAD OF THE PORT.....	2639
125.2.9	CONFIGURE CAMPUS-WIDE MTU .....	2641
125.2.10	CONFIGURE HELLO PACKET SENDING INTERVAL .....	2642
125.2.11	CONFIGURE CSNP PACKET SENDING INTERVAL.....	2643
125.2.12	CONFIGURE LSP RELATED TIME PARAMETERS .....	2644
125.2.13	CONFIGURE TO IGNORE LSP CHECKSUM ERRORS .....	2648
125.2.14	CONFIGURE SPF ALGORITHM INTERVAL.....	2648
125.2.15	CONFIGURE THE NUMBER OF DISTRIBUTION TREES.....	2649
125.2.16	TRILL MONITORING AND MAINTAINING.....	2651
<b>125.3</b>	<b>TRILL GATEWAY FUNCTION CONFIGURATION</b> .....	<b>2652</b>
125.3.1	CONFIGURE TRILL GATEWAY.....	2653
<b>125.4</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF TRILL</b> .....	<b>2654</b>
125.4.1	CONFIGURE BASIC FUNCTIONS OF TRILL.....	2654
125.4.2	CONFIGURE TRILL DRB RESOLUTION.....	2663
125.4.3	CONFIGURE DISTRIBUTION TREE ROOT RESOLUTION FOR TRILL.....	2667

125.4.4	CONFIGURE AVF VLAN SELECTION OF TRILL .....	2672
125.4.5	CONFIGURE LOAD BALANCING FOR TRILL .....	2673
<b>126</b>	<b>VXLAN .....</b>	<b>2676</b>
<b>126.1</b>	<b>OVERVIEW.....</b>	<b>2676</b>
126.1.1	BACKGROUND .....	2676
126.1.2	BASIC CONCEPTS.....	2677
126.1.3	PROTOCOL SPECIFICATION .....	2678
<b>126.2</b>	<b>VXLAN FUNCTION CONFIGURATION .....</b>	<b>2678</b>
126.2.1	CONFIGURE VXLAN INSTANCE .....	2679
126.2.2	CONFIGURE STATIC VXLAN TUNNEL .....	2685
126.2.3	CONFIGURE EVPN VXLAN TUNNEL .....	2686
126.2.4	VXLAN MONITORING AND MAINTAINING .....	2692
<b>126.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF VXLAN .....</b>	<b>2694</b>
126.3.1	CONFIGURE STATIC VXLAN FOR TWO-LAYER INTERCOMMUNICATION .....	2694
126.3.2	CONFIGURE BGP EVPN VXLAN FOR TWO-LAYER INTERCOMMUNICATION .....	2699
126.3.3	CONFIGURE STATIC CENTRALIZED VXLAN GATEWAY .....	2705
126.3.4	CONFIGURE BGP EVPN VXLAN CENTRALIZED ACTIVE-ACTIVE GATEWAY .....	2713
126.3.5	CONFIGURE BGP EVPN VXLAN DISTRIBUTED GATEWAY .....	2725
126.3.6	CONFIGURE BGP EVPN CROSS-DATA CENTER DISTRIBUTED GATEWAY.....	2738
<b>127</b>	<b>NLB.....</b>	<b>2740</b>
<b>127.1</b>	<b>OVERVIEW.....</b>	<b>2740</b>
<b>127.2</b>	<b>NLB FUNCTION CONFIGURATION .....</b>	<b>2740</b>
127.2.1	CONFIGURE NLB.....	2740
127.2.2	NLB MONITORING AND MAINTAINING .....	2742
<b>127.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF NLB .....</b>	<b>2742</b>

# 1 System Operation Basics

---

## 1.1 Overview

System operation basics mainly describe the basic knowledge of device operations, including system operation basic functions, device configuration modes, command modes, and command line interface.

## 1.2 System Operation Basic Functions

Table 1-1 System Operation Basic Function Configuration List

Configuration Task	
Device configuration mode	Device configuration mode
Command operating mode	Command operating mode
Command line interface	Command line interface

### 1.2.1 Device configuration mode

Users can log in to the device for configuration and management in different modes. (For details of the login modes, please refer to the section on "System Login" in the User Manual) The device provides five typical configuration modes:

- Logging in to the device locally through the Console port. By default, users can configure the device directly in this mode.
- Logging in to the device by remote dial-up through a Modem. The device cannot be configured directly in this mode. That is, before configuration, some preparations need to be made.
- Logging in to the device remotely through Telnet. The device cannot be configured directly in this mode. That is, before configuration, some preparations need to be made.
- Logging in to the device remotely through SSH. The device cannot be configured

directly in this mode. That is, before configuration, some preparations need to be made.

- Logging in to the device remotely through WEB. The device cannot be configured directly in this mode. That is, before configuration, some preparations need to be made.

## 1.2.2 Command operating mode

The device provides a command processing subsystem for management and execution of system commands. The subsystem shell provides the following main functions:

- Registration of system commands
- Editing of system configuration commands by users
- Parsing of the commands that have been inputted by users
- Execution of system commands

If a user configures the device through shell commands, the system provides multiple operating modes for the execution of the commands. Each command mode supports specific configuration commands. In this way, hierarchical protection is provided to the system, protecting it from unauthorized access.

The shell subsystem provides multiple modes for the operating of configuration commands. These modes have different system prompts, prompting the current system mode of the user. The following lists common configuration modes:

- Common user mode (user EXEC)
- Privileged user mode (privilege EXEC)
- Global configuration mode (global configuration)
- Interface configuration mode (interface configuration)
- File system configuration mode (file system configuration)
- Access list configuration mode (access list configuration)
- Other configuration modes (They will be described in the related sections and chapters.)

The following table shows how to enter the common command modes and switch over between the modes.

Table 1-2 System Modes and Methods of Switching Over Between the Modes

Mode	How to Enter the Mode	System Prompt	How to Exit the Mode	Functions
Common user mode	Log in to the device.	Hostname>	Run the <b>exit</b> command to exit the mode.	·Change the terminal settings ·Perform basic tests.

Mode	How to Enter the Mode	System Prompt	How to Exit the Mode	Functions
				·Display the system information
Privileged user mode	In common user mode, run the <b>enable</b> command.	Hostname#	Run the <b>disable</b> or <b>exit</b> command to exit to the common user mode.	·Configure the operating parameters of the device ·Display the operating information of the device
Global configuration mode	In privileged user mode, run the configure terminal command.	Hostname(config)#	Run the <b>exit</b> command to exit to the privileged user mode.	·Configure the global parameters that are required for the device operation
Interface configuration mode	In global configuration mode, run the <b>interface</b> command (while specifying the corresponding interface or interface group).	Hostname(config-if-xxx[number])# or Hostname(config-if-group[number])#	Run the <b>exit</b> command to exit to the global configuration mode.  Run the <b>end</b> command to exit to the privileged user mode.	In this mode, configures device interfaces, including: ·Interfaces of different types ·Interface groups
File system configuration mode	In the privileged user mode, run the <b>filesystem</b> command.	Hostname(config-fs)#	Run the <b>exit</b> command to exit to the privileged user mode.	·Manage the file system of the device
Access list configuration	In global configuration mode, run the <b>ip</b>	Hostname(config-std-nacl)#	Run the <b>exit</b> command to exit to the global	Configures the Access Control List (ACL). The configuration tasks include:

Mode	How to Enter the Mode	System Prompt	How to Exit the Mode	Functions
configuration mode	<b>access-list standard</b> or <b>ip access-list extended</b> command.	Hostname(configuration-ext-nacl)#	configuration mode.  Run the <b>end</b> command to exit to the privileged user mode.	·Configure standard access control list  ·Configure extended access control list

---

## Note

- Hostname is the system name. In global configuration mode, a user can run the **hostname** command to modify the system name, and the modification takes effect immediately.
  - If a user is not in privileged user mode while the user wants to run a privileged mode command, the user can use the do command to run the required command without the need to returning back to the privileged mode. (For details, refer to the related sections in "System Operation Basics" of the command manual.) Note that the mode switchover command such as *do configure terminal* is not included.
- 

### 1.2.3 Command line interface

The command line interface is a man-machine interface that is provided by the shell subsystem to configure and use the device. Through the command line interface, users can input and edit commands to perform the required configuration tasks, and they can also query the system information and learn the system operation status.

The command line interface provides the following functions for the users:

- System help information management
- System command inputting and editing
- History command management
- Terminal display system management

#### Command Line Online Help

The command line provides the following types of online help:

- help
- Full help

- Partial help

Through the above types of online help, users can obtain various help information. The following gives some examples.

- To obtain a brief description of the online help system, enter the **help** command in any command mode.

```

Hostname#help
Help may be requested at any point in a command by entering
a question mark '?'. If nothing matches, the help list will
be empty and you must backup until entering a '?' shows the
available options.
Two styles of help for command are provided:
1. Full help is available when you are ready to enter a
  command argument (e.g. 'show ?') and describes each possible
  argument.
2. Partial help is provided when an abbreviated argument is entered
  and you want to know what arguments match the input
  (e.g. 'show pr?'.)
And "Edit key" usage is the following:
CTRL+A -- go to home of current line
CTRL+E -- go to end of current line
CTRL+U -- erase all character from home to current cursor
CTRL+K -- erase all character from current cursor to end
CTRL+W -- erase a word on the left of current cursor
CTRL+R -- erase a word on the right of current cursor
CTRL+D,DEL -- erase a character on current cursor
BACKSPACE -- erase a character on the left of current cursor
CTRL+B,LEFT -- current cursor backward a character
CTRL+F,RIGHT -- current cursor forward a character

```

- To list all commands and their brief description in any command mode, type "?" in the command mode.

```

Hostname#configure terminal
Hostname(config)#?
aaa          Authentication, Authorization and Accounting
access-list  Access List
alarm        Set alarm option of system
arl          Address translation item
arp          Set a static ARP entry
arp-security To CPU arp security
autosave    Auto save the startup configuration
banner       Define a login banner
bgp          BGP information
cable-diagnostics Cable Diagnostics on physical interface
.....

```

- Type a command followed by "?", and all sub-commands that can be executed in the current mode are displayed.

```

Hostname#show ?
access-list  List access lists
acl-object   Show acl object
arl          Address translation item
arp          Command arp
arp-security To CPU arp security
bfd          BFD Protocol information
bgp          BGP information
cable-diagnostics Cable Diagnostics on physical interface
card_list    Show information of hardware modules
clock        Print system clock information

```

```

cluster      Config cluster
cpu          Show CPU use per process

```

- Type a character string followed by "?", and all the key words starting with the character string and their description are displayed.

```

Hostname#show a?
access-list  List access lists
acl-object  Show acl object
arl         Address translation item
arp         Command arp
arp-security To CPU arp security

```

### Command Line Error Messages

For all commands that are typed by users, the command line performs a syntax check. If the commands pass the syntax check, they are executed properly; otherwise, the system reports error messages to the users. The following table shows common error messages.

Table 1-3 Command Line Error Messages

Error Message	Error Cause
% Invalid input detected at '^' marker.	No command or key word is found, the parameter type is incorrect, or the parameter value is not within the valid range.
Type "**** ?" for a list of subcommands or % Incomplete command	The inputted command is incomplete.
Hostname#wh % Ambiguous command: wh % Please select: whoami who	The inputted character string is a fuzzy command.

### History Commands

The command line interface provides a function that is similar to the Doskey function. The system automatically saves the user inputted commands into the history command cache. Then, users can invoke the history commands saved by the command line interface at any time and execute the command repeatedly, reducing unnecessary efforts in re-typing the commands. The command line interface saves up to 10 commands for each user that is connected to the device. Then, new commands overwrite old ones.

Table 1-1 Accessing History Commands of the Command Line Interface

To...	Press...	Execution Result
Access the previous history command	The up arrow key ↑ or Ctrl+P keys	If an earlier history command is available, it is displayed. If no earlier history command is available, an alarm sound is played.
Access the next history command	The down arrow key ↓ or Ctrl+P keys	If a later history command is available, it is displayed. If no later command is available, the commands are cleared, and an alarm sound is played.

## Note

- If you want to access history commands by using the up and down arrow keys, when you telnet to the device in the Windows 98 or Windows NT OS, set Terminals > Preferred Options > Simulation Options to VT-100/ANSI.
- History command display is based on the current command mode. For example, if you are in privileged mode, only history commands in privileged mode are displayed.

## Editing Features

The command line interface provides basic command editing functions. It supports multi-line editing. Each line of command can contain up to 256 characters. The following table lists the basic editing functions that are provided by the shell subsystem for the command line interface.

Table 1-4 Basic Editing Functions

Press...	Function
A common key	If the edit buffer is not full, the character is inserted to the position of the cursor, and the cursor moves to the right. If the edit buffer is full, an alarm sound is played.
The Backspace key	Deletes the character before the cursor and moves the cursor backward. If the cursor reaches the beginning of the command, an alarm sound is played.

Press...	Function
The Delete key	Deletes the character behind the cursor. If the cursor reaches the end of the command, an alarm sound is played.
The left arrow key ← or Ctrl+B keys	Moves the cursor one characters to the left. If the cursor reaches the beginning of the command, an alarm sound is played.
The right arrow key → or Ctrl+F keys	Moves the cursor one characters to the right. If the cursor reaches the end of the command, an alarm sound is played.
The up and down arrow keys ↑↓	Display history commands.
Ctrl+A	Moves the cursor to the beginning of the command line.
Ctrl+E	Moves the cursor to the end of the command line.
Ctrl+U	Deletes all characters on the left of the cursor till the beginning of the command line.

## Display Features

To facilitate users, the command line interface provides the following display features:

If the information to be displayed is more than one screen, the pause function is provided, and the prompt "---MORE---" is displayed at the lower left corner of the screen. At this time, the options displayed in the following table are available for users.

Table 1-5 Display Features

Press...	Function
Space key, down arrow key ↓, or Ctrl-F	Display the next screen.
The up arrow key ↑ or Ctrl-B keys	Display the previous screen.
The Enter key, right arrow key → or equal key =	Scroll the displayed information one line down.
The left arrow key ← or the minus key-	Scroll the displayed information one line up.

Press...	Function
Ctrl-H	Returns back to the topmost part of the displayed information.
Any other keys	Exits the display. Then, the information that has not been displayed will not be displayed.

# 2 System Login

---

## 2.1 Overview

The device supports the following system login modes:

- Logging into the device through the Console port for management and maintenance.
- Telnet (remote login). Users can manage and maintain the device remotely in this mode.
- Secure Shell (SSH). Through its encryption and authentication technology, SSH provides secure remote login management services for users.
- WEB (remote login). Users can manage and maintain the device remotely in this mode.

## 2.2 System Login Function Configuration

Table 2-1 System Login Function Configuration List

Configuration Task	
Logging in to the device through the Console port	-
Logging in to the device through the AUX port	-
Configuring remote login through Telnet	Enable the Telnet service of the device.
	The device acts as a Telnet client for remote login.
Configuring remote login through SSH	Enable the SSH service of the device.

Configuration Task	
	The device acts as an SSH client for remote login.
Configure remote login through WEB.	Configure remote login through HTTP.
	Configure remote login through HTTPS.

### Note

- For user configuration related to Telnet and SSH remote login, refer to the section on "login control and management".

## 2.2.1 Logging in to the device through the Console port

To connect a terminal to the device through the Console port to configure the device, perform the following steps:

Step 1: Select a terminal.

The terminal can be a terminal with a standard RS-232 serial port or an ordinary PC, and the latter one is more frequently used. If the remote dial-up login mode is selected, two Modems are required.

Step 2: Connect the physical connection of the Console port.

Ensure that the terminal or the device that provides the Console port has been powered off, and then connect the RS-232 serial port of the terminal to the Console port of the device. The following figure shows the connection.



Figure 2-1 Connection for Login via the Console Port

Step 3: Configure the HyperTerminal.

After powering on the terminal, you need to set the communication parameters of the terminal, that is, baud rate of 9600 bps, 8 data bits, 1 stop bit, no parity check, and no data stream control. For a PC with the Windows XP or Windows NT OS, run the HyperTerminal program, and set the communication parameters of the serial port of the HyperTerminal according to the previously mentioned settings. The following takes the HyperTerminal in the Windows NT OS for example.

- Create a connection:

Input a connection name, and select a Windows icon for the connection.



Figure 2-2 Creating a Connection

- Select a serial communication port:

According to the serial communication port that has been connected, select COM1 or COM2.



Figure 2-3 Selecting a Serial Communication Port

- Configure parameters for the serial communication port:

Baud rate: 9600 bps

Data bit: 8 bits

Parity check: None

Stop bit: 1 bit

Data stream control: None

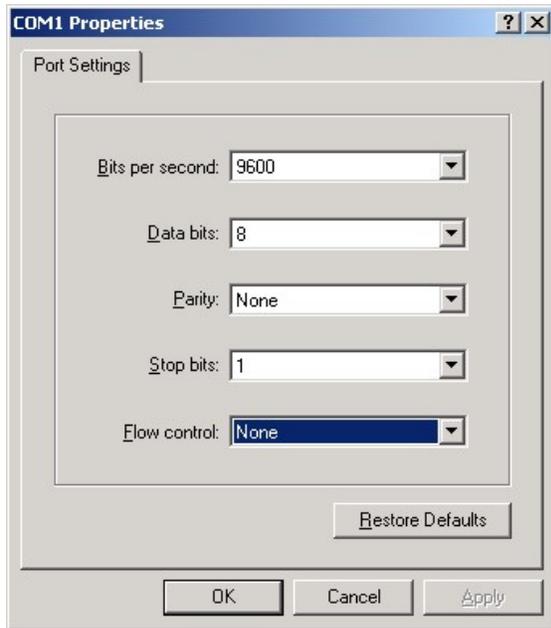


Figure 2-4 Configuring Parameters for the Serial Communication Port

- Login success authentication:

After the device with the Console port is powered on, the startup information of the device is displayed on the terminal. After the startup is completed, the "Press any key to start the shell!" message is displayed. If login authentication is configured to be required, input the user name and password; otherwise, press any key to log in directly. After the login succeeds, the "Hostname>" prompt is displayed on the terminal. Then, you can configure the device.

## 2.2.2 Configuring remote login through Telnet

### Configuration Condition

None

### Enable the Telnet service of the device.

A user can log in to the device remotely through Telnet for management and maintenance. Before using the Telnet service, enable the Telnet service of the device. After the Telnet service of the device is enabled, the Telnet service port 23 is monitored.

Table 2-2 Enabling the Telnet Service of the Device

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable the Telnet service of the device.	<b>telnet server enable</b>	Mandatory By default, the Telnet service is enabled.

**The device acts as a Telnet client for remote login.**

The user takes the device as a Telnet client to log in to the specified Telnet server for configuration and management.

Table 2-3 Taking the Device as a Telnet Client for Remote Login

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable the Telnet client of the device.	<b>telnet client enable</b>	Optional By default, the Telnet client is enabled.
The device acts as a Telnet client for remote login.	<b>telnet [ vrf vrf-name ] { hostname   remote-host } [ port-number ] [ ipv4   ipv6 ] [ source-interface interface-name ]</b>	Mandatory

---

 **Note**

- The Telnet client can log in to a remote device only when the Telnet server function of the remote device is enabled, and the network between the Telnet client and the remote device is normal.
-

## 2.2.3 Configuring remote login through SSH

### Configuration Condition

None

### Enable the SSH service of the device.

After the SSH server of a device is enabled, the device accepts the connection request initiated by the user from the SSHv1 or SSHv2 client. After the client passes the authentication, the client can access the device. After the SSH service of the device is enabled, the SSH service port 22 is monitored. If the **ip ssh server** command is configured without parameter **sshv1-compatible**, it indicates that an SSH client can log in only through SSHv2.

Table 2-4 Enabling the SSH Service of the Device

Step	Command	Description
Enter the global configuration mode.	<b>config terminal</b>	-
Enable the SSH service of the device.	<b>ip ssh server</b> [ <i>listen-port</i> ][ <b>sshv1-compatible</b> ] [ <i>listen-port</i> ]	Mandatory By default, the SSH service is disabled.

### The device acts as an SSH client for remote login.

The device acts as an SSH client to log in to the specified SSH server remotely through the SSHv1 or SSHv2 protocol. During the login, a user name and a password are required for authentication from the SSH server.

Table 2-5 Taking the Device as a Telnet Client for Remote Login

Step	Command	Description
The device acts as an SSH client for remote login.	<b>ssh</b> [ <i>vrf vrf-name</i> ] <b>version</b> { <b>1</b>   <b>2</b> } <i>remote-host port-number</i> [ <b>source-interface</b> <i>interface-name</i> ] <i>user auth-method 1 password</i>	Mandatory



- 
- The Telnet client can log in to a remote device only when the SSH service of the remote device is enabled, and the network between the SSH client and the remote device is normal.
- 

### The Device Acts as an SFTP Client to Access SFTP Server

The device acts as an SFTP client to log in to a specified SFTP server remotely through the SSHv2 protocol. During the login, a user name and a password are required for authentication from the SFTP server. The SFTP client can download files from the SFTP server or upload files to the SFTP server upon successful login.

Table 2-6 Taking the Device as an SFTP Client to Access SFTP Server

Step	Command	Description
The Device Acts as an SFTP Client to Access SFTP Server	<b>sftp {get   put} [ vrf vrf-name ] remote-host port-number [ source-interface interface-name ] user password src-filename dst-filename [compress]</b>	Mandatory

---

### Note

- The SFTP client can log in to a remote device only when the SSH service of the remote device is enabled, and the network between the SFTP client and the remote device is normal.
- 

### 2.2.4 Configure remote login through WEB.

To facilitate the configuration and maintenance of network devices, the device provides WEB-based network management function. The device provides a built-in WEB server that allows you to log in to the device from PC and use the WEB interface to configure and maintain the device directly.

The device supports two login modes for the built-in WEB server: HTTP login mode and HTTPS login mode.

The device supports IPv4 WEB login and IPv6 WEB login.

#### Configuration Condition

None

#### Configure remote login through HTTP.

A user can log in to the device remotely through HTTP for management and maintenance. Before logging in to the HTTP device via HTTP, enable the HTTP service of the device.

Table 2-7 Configuring Login Through HTTP

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable the HTTP server.	<b>ip http server</b>	Mandatory By default, the WEB server is not enabled.
Configure the HTTP server port.	<b>ip http port <i>port_number</i></b>	Optional By default, the HTTP server port number is 80.

---

 **Note**

Before starting the HTTP server, copy the corresponding WBROM files to /flash.

---

**Configure remote login through HTTPS.**

A user can log in to the device remotely through HTTPS for management and maintenance. Before logging in to the HTTPS device via HTTP, enable the HTTPS service of the device.

Table 2-8 Configuring Login Through HTTPS

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable the HTTP server.	<b>ip http server</b>	Mandatory By default, the WEB server is not enabled.
Enable the HTTPS server.	<b>ip http secure-server</b>	Mandatory By default, the WEB server is not enabled.

Step	Command	Description
Configure the HTTPS server port.	<b>ip http port</b> <i>port_number</i>	Optional By default, the HTTPS server port number is 443.
Configure certificates used in the HTTPS service.	<b>ip http certificate</b> <i>ca-store</i>	Optional By default, the HTTPS service uses self-signed certificate.

---

### Note

For the configuration of trust domain and certificate import, please refer to the section on "PKI".

---

## 2.2.5 System Login Monitoring and Maintaining

Table 2-9 System Login Monitoring and Maintaining

Command	Description
<b>show fingerprint</b>	Display the fingerprint information of the SSH public key.
<b>show ip http</b>	Display the WEB configuration information.
<b>show ip http login-user</b>	Display the user information after successful WEB login.
<b>show ip http restricted-user</b>	Display the user information after failed WEB login.
<b>show ip http statistics</b>	Display the WEB server statistics information.

## 2.3 Typical Configuration of System Login Example.

### 2.3.1 Configure a Local Terminal to Telnet to the Device.

#### Network Requirements

- A PC is used as a local terminal to log in to the device through Telnet.
- A route must be available between the PC and the device.

#### Network Topology



Figure 2-5 Network Topology for Configuring a Local Terminal to Telnet to the Device

#### Configuration Steps

Step 1: Create Virtual Local Area Networks (VLANs), and add ports to the required VLANs. (Omitted)

Step 2: Configures IP addresses for the ports. (Omitted)

Step 3: Configure the enable password.

```
Device#configure terminal
Device(config)#enable password admin
```

Step 4: Telnet to the device.

#On the PC, run the Telnet program, and input the IP address of VLAN 2.

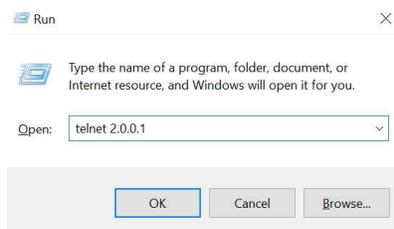


Figure 2-6 Telnet to the Device on PC

Step 5: Check the result.

#If the login succeeds, a window as shown in the following figure is displayed.

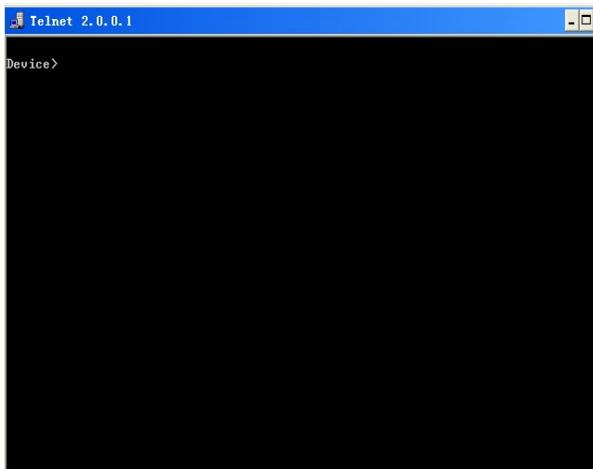


Figure 2-7 Window Displayed after Telnet Success

After logging in to the device Device successfully, input the correct enable password to obtain the required operation rights of the device. To log out of the device, input the exit command continuously.

---

### Note

- If the "Too many clients or invalid access" message is displayed, it indicates that the number of login users has reached the maximum allowed number of login users of the device. In this case, wait a while and try to log in again.
  - If the "%enable operation is locked by login-secure service" message is displayed, it indicates that the number of enable password input errors exceeds the number of continuous login authentication failures. If the number of enable password input errors reaches the number specified by the system, the system rejects the login connection request from the IP address during the specified time.
  - If the "Password required, but none set" message is displayed, it indicates that no login password has been configured.
- 

## 2.3.2 Configure a Local Device to Log in to a Remote Device via Telnet

### Network Requirements

- The local device Device1 acts as the Telnet client, while the remote device Device2 acts as the Telnet server.
- A route must be available between the two devices.
- The PC can normally log in to Device1.

### Network Topology

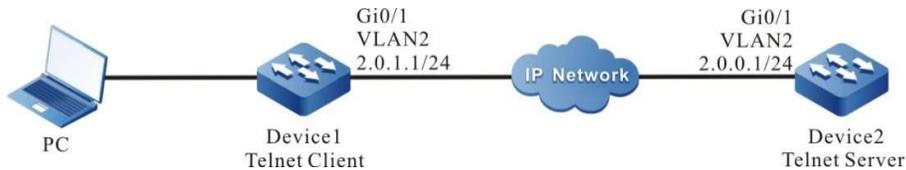


Figure 2-8 Network Topology for Configuring a Local Device to Telnet to a Remote Device

### Configuration Steps

- Step 1: Create Virtual Local Area Networks (VLANs), and add ports to the required VLANs. (Omitted)
- Step 2: Configures IP addresses for the ports. (Omitted)
- Step 3: Log in to Device1 through the PC. (Omitted)
- Step 4: On Device1, run the following command to Telnet to Device2.

```
Device1#telnet 2.0.0.1
```

#Enter the shell screen of Device2.

```
Connect to 2.0.0.1 ...done
Device2>
```

After logging in to the device Device2 successfully, input the correct enable password to obtain the required operation rights of the device. To log out of the device, input the exit command continuously.

---

### Note

- If the "Too many clients or invalid access" message is displayed, it indicates that the number of login users has reached the maximum allowed number of login users of the device. In this case, wait a while and try to log in again.
  - If the "%enable operation is locked by login-secure service" message is displayed, it indicates that the number of enable password input errors exceeds the number of continuous login authentication failures. If the number of enable password input errors reaches the number specified by the system, the system rejects the login connection request from the IP address during the specified time.
  - If the "Password required, but none set" message is displayed, it indicates that no login password has been configured within line vty.
- 

## 2.3.3 Configure a Local Device to Log in to a Remote Device via SSH

### Network Requirements

- The local device Device1 acts as the SSH client, while the remote device Device2 acts as the SSH server.
- A route must be available between the two devices.
- The PC can normally log in to Device1.

### Network Topology

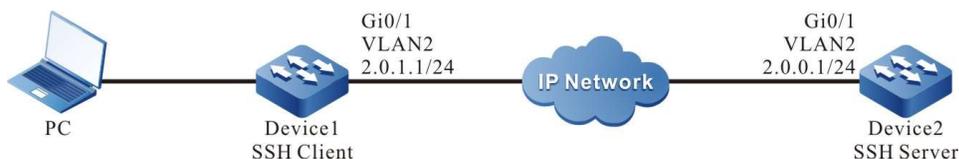


Figure 2-9 Network Topology for Configuring a Local Device to Log in to a Remote Device via SSH

### Configuration Steps

- Step 1: Create Virtual Local Area Networks (VLANs), and add ports to the required VLANs. (Omitted)
- Step 2: Configures IP addresses for the ports. (Omitted)
- Step 3: Configure a local user and the related properties.

#Configure the user name and password of Device2.

```
Device2#configure terminal
Device2(config)#local-user admin1 class manager
Device2(config-user-manager-admin1)#service-type ssh
Device2(config-user-manager-admin1)#password 0 admin1
Device2(config-user-manager-admin1)#exit
```

- Step 4: Enable the SSH server function of Device2.

```
Device2(config)#ip ssh server
```

- Step 5: Set the login authentication mode to local authentication.

```
Device2(config)#line vty 0 15
Device2(config-line)#login aaa
Device2(config-line)#exit
```

- Step 6: #On Device1, log in to Device2 through SSH.

#Configure Device1 to log in to Device2 through SSH.

```
Device1#ssh version 2 2.0.0.1 22 admin1 auth-method 1 admin1
The authenticity of host '2.0.0.1' can't be established
RSA key fingerprint is 7b:ed:cc:81:cf:12:36:6f:f7:ff:29:15:63:75:64:10.
Are you sure you want to continue connecting (yes/no)? yes
Device2>
```

- Step 7: Check the result.

If the login succeeds, the shell screen of Device2 is displayed.

---

## Note

- If the "Connection closed by foreign host" message is displayed, it indicates that the SSH service of the peer end is disabled, or the inputted user name or password is incorrect.
  - The SSH server can be configured not to use authentication. If the SSH server does not use authentication, when a client logs in, a user can use any character string as the user name and password.
- 

### 2.3.4 Configure a Device as an SFTP Client

#### Network Requirements

- Take the PC as an SFTP server, and the device acts as an SFTP client. The network between the server and the device is normal.
- On the SFTP server, the user name for a device to log in to the FTP server is admin, and the password is admin. The files to be downloaded are placed in the SFTP server directory.
- The device acts as the SFTP client to upload files to and download files from the SFTP server.

#### Network Topology



Figure 2-10 Network Topology for Configuring the Device as an SFTP Client

#### Configuration Steps

- Step 1: Create Virtual Local Area Networks (VLANs), and add ports to the required VLANs. (Omitted)
- Step 2: Configure an SFTP server, and place the files to be downloaded in the SFTP server directory. (Omitted)
- Step 3: Configure the IP addresses of the devices so that the network between the client and the server is normal. (Omitted)

Step 4: Device acts as the SFTP client to upload files to and download files from the SFTP server.

#Download a file from the SFTP server to the file system of the device.

```
Device#sftp get 2.0.0.1 22 admin admin sp8-g-6.6.7(46)-dbg.pck sp8-g-6.6.7(46)-dbg.pck
The authenticity of host '2.0.0.1 (2.0.0.1)' can't be established.
RSA key fingerprint is e4:dd:11:2e:82:34:ab:62:59:1c:c8:62:1d:4b:48:99.
Are you sure you want to continue connecting (yes/no)? yes

Downloading#####
#####OK!
```

#Upload the startup file in the file system of Device to the SFTP server.

```
Device#sftp put 2.0.0.1 22 admin admin startup startup.txt
The authenticity of host '2.0.0.1 (2.0.0.1)' can't be established.
RSA key fingerprint is e4:dd:11:2e:82:34:ab:62:59:1c:c8:62:1d:4b:48:99.
Are you sure you want to continue connecting (yes/no)? yes

Uploading#####
#####OK!
```

Step 5: Check the result.

#After the copy process is completed, check whether the downloaded file exists in the file system of the device. In the SFTP server, check whether the uploaded file exists. (Omitted)

```
Device(config-fs)#dir
size  date  time  name
-----
101526  MAR-01-2015  01:17:18  logging
10147  MAR-26-2015  07:58:50  startup
10207  MAR-01-2015  01:17:54  history
11676148  MAR-26-2013  07:51:32  sp8-g-6.6.7(46)-dbg.pck
2048  JAN-10-2015  17:30:20  snmp      <DIR>
```

## 2.3.5 Configure a Device as an SFTP Server

### Network Requirements

- The device acts as an SFTP server, while PC acts as an SFTP client. The network between the client and the server is normal.
- On the SFTP server Device, the user name is admin1, and the password is admin1. The file system directory of the device acts as the root directory of the SFTP server.
- The PC acts as the SFTP client to upload files to and download files from the SFTP server device.

### Network Topology



Figure 2-11 Network Topology for Configuring the Device as an SFTP Server

### Configuration Steps

- Step 1: Create Virtual Local Area Networks (VLANs), and add ports to the required VLANs. (Omitted)
- Step 2: Configure IP addresses for the ports so that the network between the PC and the device is normal. (Omitted)
- Step 3: On Device, enable the SFTP service, and configure the authorized user name and password.

#On the SFTP server Device, configure the authorized user name and password.

```
Device#configure terminal
Device(config)#local-user admin1 class manager
Device(config-user-manager-admin1)#service-type ssh
Device(config-user-manager-admin1)#password 0 admin1
Device(config-user-manager-admin1)#exit
```

#Enable SSH service on Device (SFTP is a sub-module of the SSH protocol)

```
Device(config)#ip ssh server
```

- Step 4: The PC acts as the SFTP client to upload files to and download files from the SFTP server Device.

#In the following part, the Linux system is taken as an example to illustrate the process.

#Input the correct IP address, user name, and password to log in to the SFTP server.

```
[root@aas ~]# sftp admin1@2.1.1.1
Connecting to 2.1.1.1...
admin@2.1.1.1's password:
sftp>
```

#Obtain the startup file in the file system of the SFTP server Device.

```
sftp> get startup startup
Fetching /flash/startup to startup
/flash/startup                               100% 13KB 12.9KB/s 00:00
```

#After the file copy process is completed, the file is available in the specified operation directory.

```
sftp> ls
sp8-g-6.6.7(74)-dbg.pck sp8-g-6.6.7(76)-dbg.pck startup      tech      test_pc
sftp>
```

#Upload the files in the PC to the file system of SFTP server Device.

```
sftp> put sp8-g-6.6.7(76)-dbg.pck sp8-g-6.6.7(76)-dbg.pck
Uploading sp8-g-6.6.7(76)-dbg.pck to /flash/ sp8-g-6.6.7(76)-dbg.pck
sp8-g-6.6.7(76)-dbg.pck 100% 11424KB 16.0KB/s 00:00
```

#After the file copy process is completed, the file is available in the file system of the device.

```
Device(config-fs)#dir
size      date      time      name
-----
2048      JUN-30-2015 16:35:50 tech      <DIR>
10229     JUN-12-2015 14:31:22 history
101890    JUN-30-2015 17:46:40 logging
39755     JUN-30-2015 16:33:56 startup
740574    MAY-27-2014 18:55:14 web-Spl-1.1.243.rom
2048      JUN-27-2015 16:26:10 snmp      <DIR>
11698172  JUN-30-2015 10:36:18 sp8-g-6.6.7(76)-dbg.pck
```

### 2.3.6 Configure a Local Device to Log in to a Remote Device via SSH Public Key Authentication

#### Network Requirements

- A PC is used as a local terminal where the SecureCRT software is installed.
- A PC is used as a local terminal to log in to the device via SSH public key.

#### Network Topology



Figure 2-12 Network Topology for Configuring a Local Device to Log in to a Remote Device via SSH Public Key Authentication

#### Configuration Steps

Step 1: Configure IP addresses for the ports and configure the routing protocol to enable intercommunication between the PC and Device. (Omitted).

Step 2: Configure SSH service and FTP function.

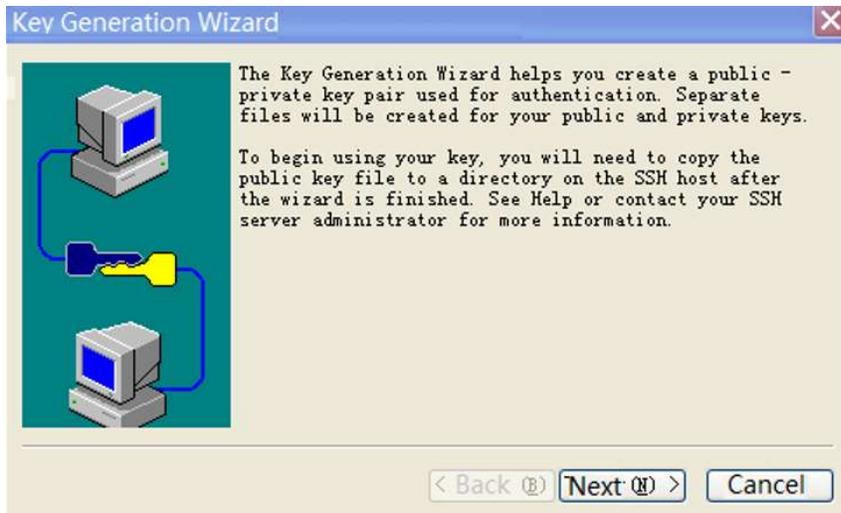
```
Device#configure terminal
Device(config)#ip ssh server
```

Step 3: Configure the login user name for Device.

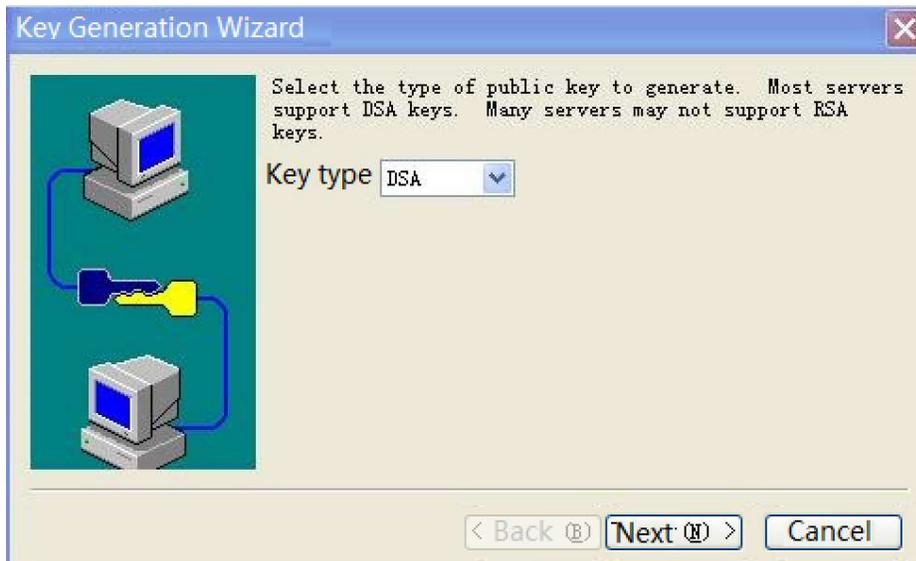
```
Device(config)#local-user user1 class manager
Device(config-user-manager-user1)#service-type ssh
Device(config-user-manager-user1)#exit
```

Step 4: Generate the SSH public key file on the PC.

# Windows operating system is used as an example herein, and Version 6.1.2 of SecureCRT is used. Open the SecureCRT software toolbar on the PC and click on "Tools", then click on "Create Public Key (C)" in the drop-down menu, the key generation wizard will pop up, click on Next.



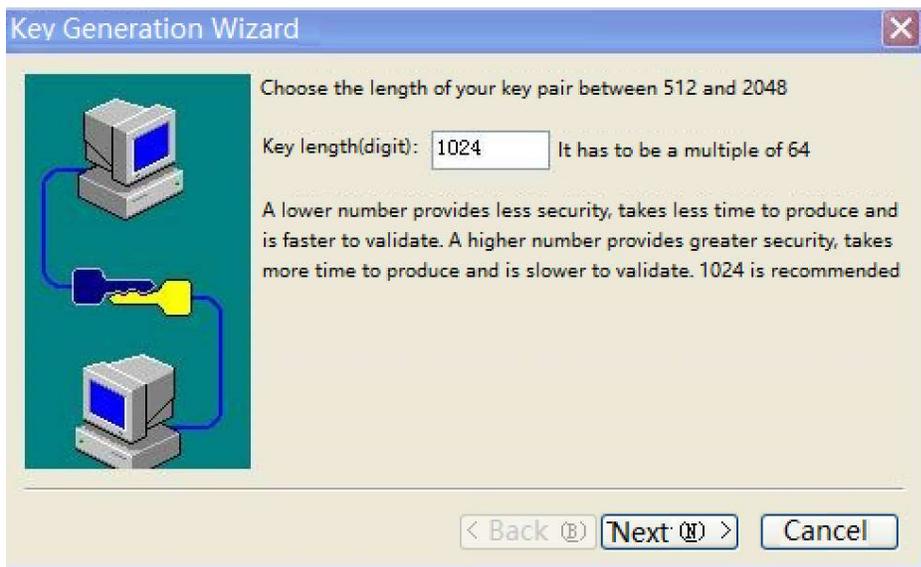
# Key type, choose either from DSA and RSA, here DSA is chosen as an example, click on Next.



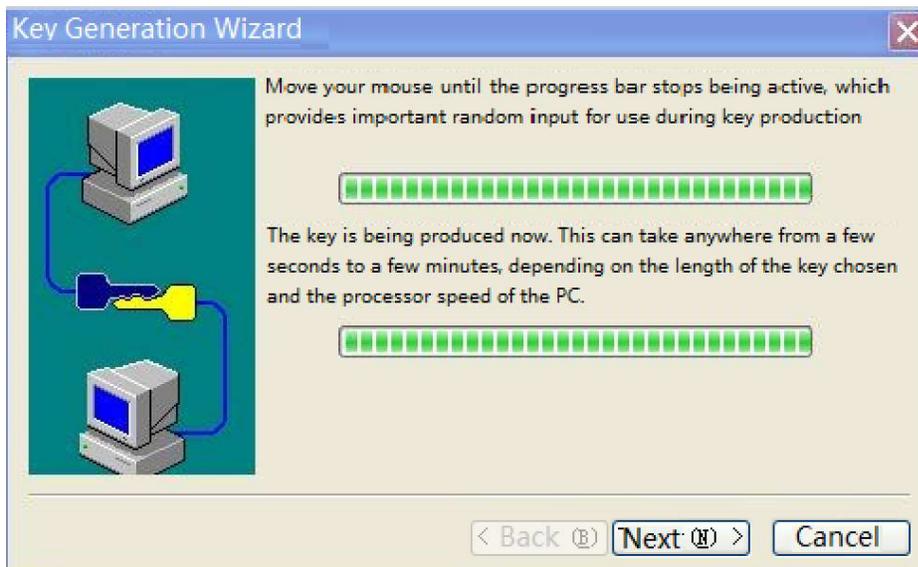
#Passphrase is locally valid and can be ignored, click on Next.



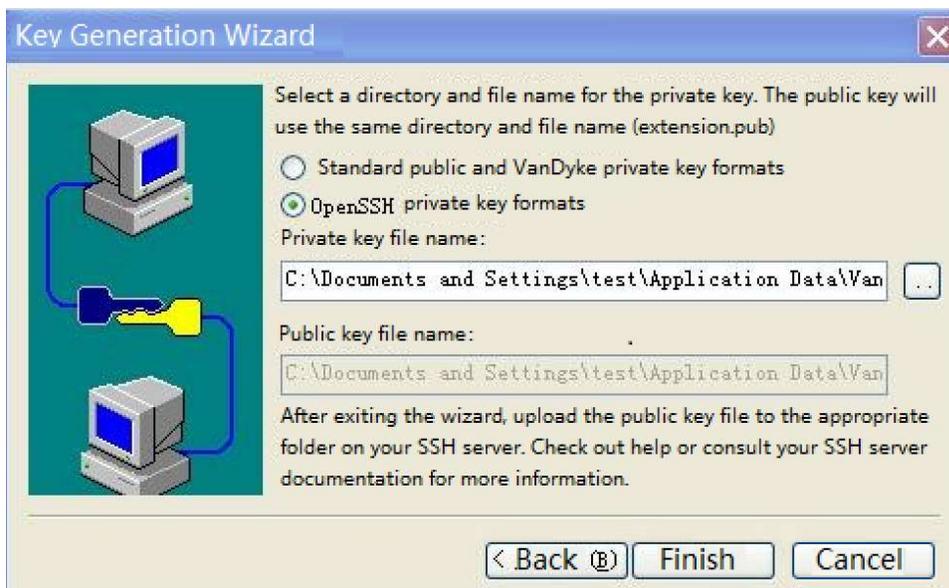
\#Key length to be filled in according to the instructions, click on Next.



#Key generation, you need to keep moving the mouse, after the key is generated, click on Next.



#Select the storage key format, note that here you must select the OpenSSH key format, click "Finish".



#Create the file "authorized\_keys" in the FTP server path of the PC, copy all the contents of the public key file "Identity.pub" to "authorized\_keys". authorized\_keys", and Device will copy the file "authorized\_keys" to the path /flash/sshpubkey/user1/.

```
Device#filesystem
Device(config-fs)#mkdir sshpubkey
Device(config-fs)#cd sshpubkey
Device(config-fs)#mkdir user1
Device(config-fs)#cd user1
Device(config-fs)#copy ftp 2.0.0.1 username password authorized_keys file-system authorized_keys
```

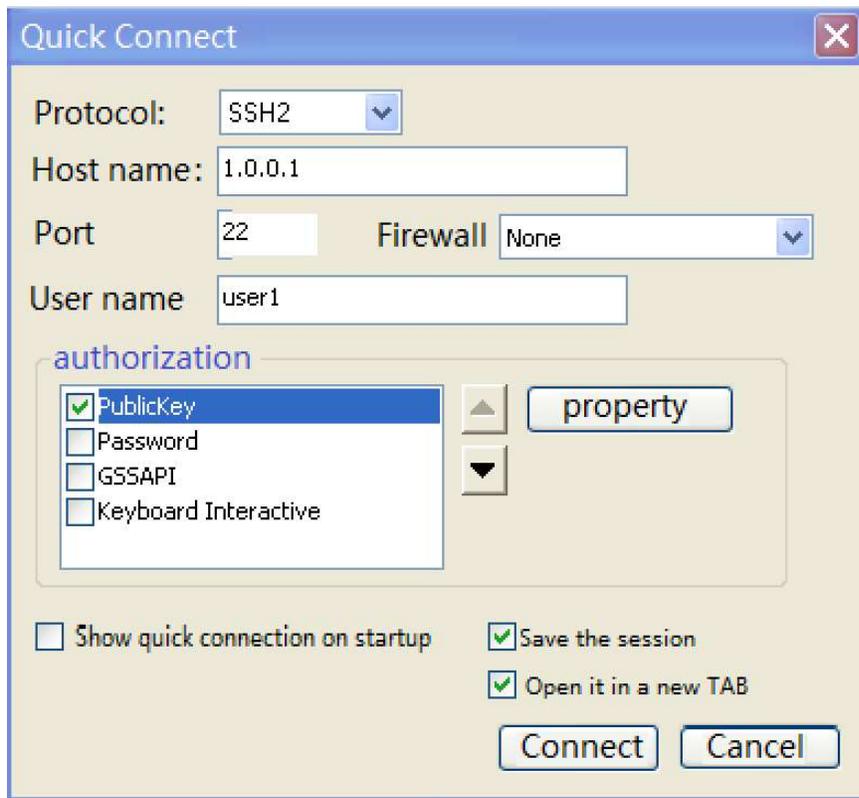
---

## Note

- OpenSSH must be selected as the storage key format, other formats are not supported.
  - When copying the content of "Identity.pub", you need to select all and then copy it without line breaks.
  - When there are multiple clients logging in with the same user name, paste another public key after the public key information stored in "authorized\_keys" in a new line, and so on.
  - By default, the device does not have the directory /flash/sshpubkey/user1/ and needs to be created in filesystem, where user1 is the user name used for authentication and the user name is the user existing on the device, if the user name is user2, then /flash/sshpubkey/user2/ needs to be created.
  - SSH public key authentication does not support SSHv1 version.
- 

Step 5: Check the result.

The PC uses SecureCRT software to establish an SSH connection, using publickey priority or unique authentication, click on "Connect" to see that the connection will not be asked for a password and can log in to the device directly.



# 3 System Control and Management

---

## 3.1 Overview

To enhance the operation security of the device, in user login or enable operation, the device provides multiple authentication management types (including AAA. Refer to the related sections and chapters in AAA configuration manual.) Only the user with the required operation rights can log in or perform the enable operation successfully.

To authorize different set of executable commands to different level of users, the device commands are divided into levels 0-15, and user levels are divided into levels 0-15. Among the levels, level 0 has the lowest rights while level 15 has the highest rights.

## 3.2 Login Control and Management Function Configuration

Table 3-1 Login Control and Management Configuration List

Configuration Task	
Switch over between user levels.	Switch over between user levels.
Configure the command level.	Configure the command level.
Configure the enable password.	Configure the enable password.
Configure users and the related properties.	Configure auto commands.
	Configure no password authentication during login.
	Configure user passwords.
	Configure the user privilege level.
Configure line properties.	Enter the line configuration mode of the Console port.

Configuration Task	
	Enter the line configuration mode of the Telnet or SSH user.
	Configure Absolute Time for Login User Operation
	Configure the privilege level of the login user.
	Configure users to automatically execute commands after login.
	Configure auto command execution options.
	Configure login user idle timeout time.
	Configure the line password.
	Configure the login authentication mode.
	Configure the line authorization mode.
	Configure the line accounting mode.
	Enable the Modem function of the Console port.
	Configure the user login timeout time.

### 3.2.1 Switch over between user levels.

If a user name and password of the corresponding level is configured, the user can run the enable level (0-15) command and then enter the correct password to enter the required user level. Meanwhile, the user has the execute permission of the user level and the lower levels.

If the current user level is higher than the user level that the user wants to enter, then no authentication is required, and the user directly enters the required user level. If the user level that the user wants to enter is higher than the current user level, authentication is required according to the current configuration, and the authentication mode is selected according to the configuration.

If the enable password of the corresponding level has been configured (by using the **enable password level** command), while the enable authentication of Authorization, Authentication and Accounting (AAA) is not configured or the AAA enable authentication is set to use the enable method, use the enable password for authentication.

If the enable password of the required level has not been configured, but the enable authentication method is set to use the local enable password for authentication, there are two cases:

a) In the case of a Telnet user, the login fails. If AAA has not been configured, the "% No password set" is prompted. If AAA has been configured, the "% Error in authentication" message is prompted.

b) For a Console port user, if AAA has been configured, try to use the enable password for authentication during the login. If the enable password has not been configured, use the none authentication method. That is, the login passes the authentication by default. If AAA has not been configured, the "% No password set" message is prompted, and the authentication fails.

If enable authentication succeeds, the user enters the specified user level and the user has execution permission of the level. To query the user level of the current user, run the **show privilege** command.

If the aaa authentication enable-method is configured and a related method list is used to enable authentication, then the related method is required for authentication, including:

a) If aaa authentication enable-method none is configured, no password is required.

b) If aaa authentication enable-method enable is configured, and the enable password is configured, use the password for authentication. Otherwise, the "% Bad passwords" message is prompted, and the authentication fails.

c) If aaa authentication enable default radius is configured, Remote Authentication Dial in User Service (RADIUS) authentication is used. Note that the enable authentication user names for RADIUS are fixed, that is, \$enable+level\$. Here "level" is a number in the range of 1-15, that is, the level that the user wants to enter. The RADIUS user names are fixed, therefore, during authentication, no user name is required. The user needs only to input the password. If passwords have been set for users of different levels on the RADIUS server, after inputting the correct password, the login succeeds; otherwise, the login fails. For example, in running the enable 10 command, the fixed user name is \$enable10\$. If the user name exists on the RADIUS server, input the password corresponding to the user name, and then the authentication succeeds.

d) If aaa authentication enable default tacacs is configured, Terminal Access Controller Access Control System (TACACS) authentication is used. If the user name is displayed during login, keep the user name for login, and input the enable password of the user name. Otherwise, input a user name and the enable password of the user name. If the inputted user name exists in the TACACS server and the enable password of the TACACS has been set, the authentication succeeds; otherwise, the authentication fails.

---

 **Note**

- The previously mentioned enable authentication methods can form a combination in use.
-

None

### Switch over between user levels.

If a user has the corresponding authority, the user can switch from the common user mode to the privileged user mode by switching over between user levels with a command. Then, the user has the authority of the user level. If a user runs the command in the privileged user mode, the user level switchover is performed according to the command parameter.

Table 3-2 Switching Over Between User Levels

Step	Command	Description
Switch over between user levels.	<b>enable</b> [ <i>level-number</i> ]	Mandatory  By default, the user level is level 15.

### 3.2.2 Configure the command level.

#### Configuration Condition

None

#### Configure the command level.

In the application program, each shell command has a default level, which can be modified through the **privilege** command. A user can execute only the commands with the level equal to or smaller than the user level. For example, a user with the user level 12 can execute only the commands with the levels 0-12. In configuring the command level, you need to make use of command modes. You can modify the level of a single command or all commands in a specified command mode.

Table 3-3 Configuring the Command Level

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the command level.	<b>privilege</b> <i>privilege-mode</i> <b>level</b> <i>level-number</i> [ <b>all</b>   <b>command</b> <i>command-line</i> ]	Mandatory

### 3.2.3 Configure the enable password.

#### Configuration Condition

None

### Configure the enable password.

The enable password is the password that is used by a level of users to enter the local level. If no level is specified in the enable command, the password is set as the enable password of level 15 by default.

Table 3-4 Configuring Enable Password

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the enable password.	<b>enable password</b> [ <b>level</b> <i>level-number</i> ] [ <b>0</b> ] <i>password</i>	Mandatory By default, no enable password is configured.

### 3.2.4 Configure line properties.

The device supports up to one Console port user and 16 Telnet or SSH users to log in at the same time. Line commands can set different authentication and authorization properties for the login users.

#### Configuration Condition

None

#### Enter the line configuration mode of the Console port.

To configure the Console port properties, you need to enter the line configuration mode of the Console port.

Table 3-5 Entering the Line Configuration Mode of the Console Port

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the line configuration mode of the Console port.	<b>line con 0</b>	Mandatory

#### Enter the line configuration mode of the Telnet or SSH user.

To configure the Telnet or SSH properties, you need to enter the line configuration mode of Telnet or SSH.

Table 3-6 Entering the Line Configuration Mode of the Telnet or SSH User

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the line configuration mode of the Telnet or SSH user.	<b>line vty</b> { <i>vtty-min-number</i> } [ <i>vtty-max-number</i> ]	Mandatory

### Configure Absolute Time for Login User Operation

The absolute time for the login user operation refer to the timeout time from the successful login of a user to the automatic exit of the user, in the unit of minute. If the absolute time is set to 0, it indicates that the time is not limited. By default, the time is 0. In addition, five seconds before the configured time expires, the following prompt message is displayed: Line timeout expired.

Table 3-7 Configuring the Absolute Time for the Login User Operation

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the line configuration mode of the Console port or Virtual Type Terminal (VTY).	<b>line</b> { <b>con 0</b>   <b>vtty</b> <i>vtty-min-number</i> [ <i>vtty-max-number</i> ] }	Mandatory
Configure the absolute time for the login user operation.	<b>absolute-timeout</b> <i>absolute-timeout-number</i>	Mandatory By default, the absolute time is 0, that is, no time limit.

### Configure Privilege Level of Login User

Configure the privilege level of the login user. The default privilege level is 1. A user can execute only the commands with the level equal to or smaller than the current level.

Table 3-8 Configuring the Privilege Level of the Login User

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Enter the line configuration mode of the Console port or Virtual Type Terminal (VTY).	<b>line</b> { <b>con 0</b>   <b>vtty</b> <i>vtty-min-number</i> [ <i>vtty-max-number</i> ] }	Mandatory
Configure the privilege level of the login user.	<b>privilege level</b> <i>level-number</i>	Mandatory  By default, the authorized user level is 1.

### Configure Access Control List

Configure the user Access Control List (ACL) so that only hosts allowed by the ACL can log in to the device.

Table 3-9 Configuring Line Access Control List

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the line configuration mode of Virtual Type Terminal (VTY).	<b>line</b> { <b>vtty</b> <i>vtty-min-number</i> [ <i>vtty-max-number</i> ] }	Mandatory
Configure Access Control List	<b>access-class</b> { <i>access-list-number</i>   <i>access-list-name</i> } { <b>in</b>   <b>out</b> }	Mandatory
Configure ipv6 ACL Control List	<b>ipv6 access-class</b> { <i>access-list-number</i>   <i>access-list-name</i> }{ <b>in</b>   <b>out</b> }	Optional

### Configure users to automatically execute commands after login.

Configure the commands to be automatically executed after users successfully log in. By default, no command is to be automatically executed.

Table 3-10 Configuring the Commands to be Automatically Executed after Successful Login

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the line configuration mode of the Console port or Virtual Type Terminal (VTY).	<b>line { con 0   vty vty-min-number [ vty-max-number ] }</b>	Mandatory
Configure the commands to be automatically executed after successful login.	<b>autocommand command-line</b>	Mandatory

### Configure auto command execution options.

You can configure delay time for auto commands, and configure whether to disconnect the user connection after the commands are executed automatically. By default, the command execution is not delayed, and the user connection is disconnected after the commands are executed automatically.

The auto command execution options include delay and whether to disconnect the user connection after command execution.

Table 3-11 Configuring Auto Command Execution Options

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the line configuration mode of the Console port or Virtual Type Terminal (VTY).	<b>line { con 0   vty vty-min-number [ vty-max-number ] }</b>	Mandatory
Configure the auto command execution options.	<b>autocommand-option { nohangup [ delay delay-time-number ]   delay delay-time-number [ nohangup ] }</b>	Mandatory

### Note

- The `autocommand-option` command is valid only after the `autocommand` function is

---

configured.

---

### Configure login user idle timeout time.

If the time in which login user does not perform any operation on the device is longer than the idle timeout time, the device make the current login user to log out. The default idle timeout exit time is 5 minutes. If the time is set to 0, then idle timeout does not take effect.

Table 3-12 Configuring the Idle Timeout Exit Time

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the line configuration mode of the Console port or Virtual Type Terminal (VTY).	<b>line { con 0   vty vty-min-number [ vty-max-number ] }</b>	Mandatory
Configuring the idle timeout exit time.	<b>exec-timeout exec-timeout-minute_number [ exec-timeout-second_number ]</b>	Mandatory The default idle timeout exit time is 5 minutes.

### Configure the line password.

Use 0 and 7 to indicate whether the line password is in plain text or cipher text. 0 indicates that the password is in plain text while 7 indicates that the password is in cipher text. In interaction mode, only plain-text password is allowed. That is, in this mode, only the parameter value 0 is used.

Table 3-13 Configuring the Line Password

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the line configuration mode of the Console port or Virtual Type Terminal (VTY).	<b>line { con 0   vty vty-min-number [ vty-max-number ] }</b>	Mandatory
Configure the line password.	<b>password 0 password</b>	Mandatory

### Configure the login authentication mode.

The device supports the following login authentication modes:

Login authentication using login password: the line password authentication is used.

Login authentication using login aaa: AAA authentication is used.

No login means that no authentication is required to log in.

Telnet uses the no login authentication mode by default, and SSH uses the local user authentication mode by default.

Table 3-14 Configuring Login Authentication Mode

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the line configuration mode of the Console port or Virtual Type Terminal (VTY).	<b>line { con 0   vty vty-min-number [ vty-max-number ] }</b>	Mandatory
Configure the login authentication mode.	<b>login {aaa [ domain-name   default]   password}</b>	This command affects AAA authentication, authorization, and billing.

#### Configure the user login timeout time.

When a user logs in to the device, if the waiting time for entering the user name or password times out, then the system will prompt a login failure. By default, the timeout time for login is 30 seconds. Users can configure the timeout time for login using this function.

Table 15-3 Configuring the Timeout Time for User Login

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the line configuration mode of the Console port or Virtual Type Terminal (VTY).	<b>line { con 0   vty vty-min-number [ vty-max-number ] }</b>	Mandatory
Configure the timeout time for user login.	<b>timeout login respond respond-time-value</b>	Mandatory By default, the time to enter the username or

Step	Command	Description
		password before the session timeout is 30 seconds.

### 3.2.5 System Control and Management Monitoring and Maintaining

Table 3-16 System Control and Management Monitoring and Maintaining

Command	Description
<b>clear line</b> { <b>con</b> <i>con-number</i>   <b>vty</b> <i>vty-number</i> }	Clear a terminal service.
<b>show privilege</b>	View the privilege level of the current user.
<b>show users</b>	Display the configured user information.

# 4 FTP, FTPS, TFTP and SFTP.

---

## 4.1 Overview

File Transfer Protocol (FTP) is used between a server and a client to transmit files. It improves file sharing, and provides an efficient and reliable data transmission mode between the user and remote computer. The FTP protocol usually uses TCP port 20 and 21 for transmission. Port 20 transmits data in active mode, and port 21 transmits control messages.

Similar to most Internet services, FTP uses the client/server communication mechanism. To connect to an FTP server, usually you are required to have the authorized account of the FTP server. On the Internet, a large number of FTP servers are anonymous FTP servers, which aim at provide file copying services to the public. For this type of FTP server, users need not register with the server or obtain authorization from the FTP servers.

FTP supports two types of file transmission modes:

- ASCII transmission mode, in which text files are transmitted.
- Binary transmission mode, in which program files are transmitted.

If the device acts as an FTP client, only the binary transmission mode is supported. If the device acts as an FTP server, both transmission modes are supported.

FTP supports two working modes:

- Active mode: An FTP client first sets up a connection with an FTP server through the TCP21 port and sends commands through this channel. If the FTP client wants to receive data, it sends the PORT command through this channel. The PORT command contains through which port the client receives data. Then the FTP server connects its TCP20 port to the specified port of the FTP client to transmit data. The FTP server must set up a new connection with the FTP client to transmit data.
- Passive mode: The method of setting up the control channel in passive mode is similar to that in active mode. However, after the connection is set up, the PASV command instead of the PORT command is sent. After the FTP server receives the PASV command, it opens a high end port (with the port number larger than 1024) and inform the client to transmit data through this port. The FTP client connects to the port of the FTP server, and then the FTP server transmits data through this port.

Many Intranet clients cannot log in to the FTP server in active mode, because the server fails to set up a new connection with an Intranet client.

When the device acts as an FTP client, it sets up a data connection in active mode.

FTPS is an enhanced FTP protocol that uses standard FTP protocols and commands at the Secure Sockets Layer (SSL), adding SSL security features to the FTP protocol and data channels. FTPS is also known as "FTP-SSL" or "FTP-over-SSL". SSL is a protocol that encrypts and decrypts data in a secure connection between a client and an SSL-enabled server. Only the FTP client on the device supports this feature. Trivial File Transfer Protocol (TFTP) is a simple file transfer protocol which is based on the User Datagram Protocol (UDP). It transmits data through UDP port 69. The protocol is designed for transmission of small files; therefore, it does not have as many functions as the FTP protocol. It does not support list of directories or authentication. The device only implements the functions of the TFTP client.

SFTP (Secure File Transfer Protocol /Secure FTP) is a new feature added in SSH 2.0. SFTP is built on top of SSH connection, which allows remote users to securely log in to the device and perform operations such as file management and file transfer, providing a higher level of security for data transfer. SFTP provides a secure method for transferring files. SFTP is a sub-function of SSH that enables secure file transfer. SFTP encrypts the transmission of authentication information and the transmitted data, so it is very safe to use SFTP. If you have high requirements for network security, SFTP can be used to replace FTP. However, since SFTP file transfer uses encryption/decryption technology, the transfer efficiency is lower than FTP file transfer.

## 4.2 FTP, FTPS, TFTP and SFTP Function Configuration

Table 4-1 FTP and TFTP Function Configuration List

Configuration Task	
Configure an FTP server.	Configure the functions of an FTP server.
Configure an FTP client.	Configure the functions of an FTP client.
Configure a TFTP client.	Configure the functions of a TFTP client.
Configure an SFTP Server	Configure the functions of an SFTP Server.
Configure an SFTP client.	Configure the functions of an SFTP client.

### 4.2.1 Configure an FTP server.

#### Configuration Condition

None

### Configure the functions of an FTP server.

Before configuring the device as the FTP server, first enable the FTP server function. Then, the FTP client can access the FTP server. For security sake, the device provides the FTP service only to authorized users, and it limits the maximum allowed number of concurrent login users.

Table 4-2 Configuring FTP Server Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable the FTP server function.	<b>ftp enable</b>	Mandatory By default, the FTP server function is disabled.
Create an user administrator and enter the user administrator mode	<b>local-user <i>user-name</i> class manager</b>	-
Configure service-type that supports FTP for users	<b>service-type ftp</b>	-
Configure user password	<b>password 0 <i>password</i></b>	Mandatory By default, the user name and password are not configured. For details of the command, refer to the section on "LUM".
Configure the FTP service listening port number	<b>ftp listen-port [ <i>port-num</i> ]</b>	Optional By default, the FTP service listening port number is 21.
Configure the maximum allowed number of concurrent login users.	<b>ftp max-user-num <i>user-num</i></b>	Optional By default, the maximum allowed number of concurrent login users is 1.
Configure the connection timeout time.	<b>ftp timeout <i>time</i></b>	Optional

Step	Command	Description
		By default, the connection timeout time is 300 seconds.

#### 4.2.2 Configure an FTP client.

##### Configuration Condition

None

##### Configure the functions of an FTP client.

On the device, when you use the copy command to **copy** files (Refer to the related sections in "File System Management") or use the **sysupdate** command to upgrade the software version (Refer to the related sections in "Software Upgrade"), the device can be triggered to act as the FTP client and set up a connection with the remote FTP server.

The connection between an FTP client and an FTP server uses the address of the outgoing interface of the route to the FTP server as the source address by default. Users can also use the **ip ftp source-address** or **ip ftp source-interface** commands to specify the FTP client source address or source interface.

Table 4-3 Configuring FTP Client Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure FTP Client Source Address.	<b>ip ftp { source-interface <i>interface-name</i>   source-address <i>ip-address</i> }</b>	Optional By default, the address of the outgoing interface of the route to the FTP server is used as the source address.
Configure the FTP Client to Use Port Mode as a Priority.	<b>ip ftp port-first</b>	Optional By default, preference is given to passive mode for establishing data connections to the server

---

 **Note**

- In some network environments, because of security factors, the communication between the address of the outgoing interface of the route to the FTP server and the FTP server may be restricted, while communication with other service interface addresses are normal. In such case, you can use the `ip ftp source-address`, `ip ftp source-interface` commands to specify the FTP client source address or source interface.
- 

### 4.2.3 Configure a TFTP client.

#### Configuration Condition

None

#### Configure the functions of a TFTP client.

On the device, when you use the **copy** command to copy files (Refer to the related sections in "File System Management") or use the **sysupdate** command to upgrade the software version (Refer to the relevant sections on "Software Upgrade"), the device can be triggered to act as the TFTP client and set up a connection with the remote TFTP server.

The connection between a TFTP client and a TFTP server uses the address of the outgoing interface of the route to the TFTP server as the source address by default. Users can also use the **ip tftp source-address** or **ip tftp source-interface** commands to specify the TFTP client source address or source interface.

Table 4-4 Configuring TFTP Client Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure TFTP Client Source Address	<b>ip tftp { source-interface <i>interface-name</i>   source-address <i>ip-address</i> }</b>	Optional By default, the address of the outgoing interface of the route to the TFTP server is used as the source address to communicate with the TFTP server.

---

 **Note**

- 
- In some network environments, because of security factors, the communication between the address of the outgoing interface of the route to the TFTP server and the TFTP server may be restricted, while communication with other service interface addresses are normal. In such case, you can use the `ip tftp source-address`, `ip tftp source-interface` commands to specify the TFTP client source address or source interface.
- 

#### 4.2.4 Configure the TFTP Server

##### Configuration Condition

None

##### Configure TFTP Server Function

Before configuring the device as the TFTP server, first enable the TFTP server function. Then, the TFTP client can access the TFTP server.

Table 4-5 Configuring TFTP Server Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable the TFTP server function.	<b>tftp enable</b>	Mandatory By default, the TFTP server function is disabled.

#### 4.2.5 Configure an SFTP Server

##### Configuration Condition

None

##### Configure the functions of an SFTP Server.

Before configuring the device as the SFTP server, first enable the SFTP server function. Then, the SFTP client can access the SFTP server. Since SFTP is a sub-function of SSH, the configuration to enable SFTP service is the same as that to enable SSH remote login service.

Table 4-6 Configuring SFTP Server Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Enable the SFTP server function.	<b>ip ssh server [ sshv1-compatible ] [ listen-port ]</b>	Mandatory By default, the SFTP server function is disabled.

#### 4.2.6 Configure an SFTP client.

##### Configuration Condition

None

##### Configure the functions of an SFTP client.

The device acts as an SFTP client and connects to the SFTP server to download files from the SFTP server or upload files to the SFTP server.

Table 4-7 Configuring SFTP Client Function

Step	Command	Description
Configure the device to act as the SFTP client to upload files to and download files from the SFTP server.	<b>sftp { get   put } [vrf vrf-name] host-ip-address port-number [source-interface interface-name] user password src-filename dest-filename [compress]</b>	Optional

#### 4.2.7 FTP and TFTP monitoring and maintaining

None

### 4.3 Typical Configuration Example of FTP and TFTP

#### 4.3.1 Configure a Device as an FTP Client

##### Network Requirements

- A PC acts as an FTP server, and the device Device acts as an FTP client. The network between the server and the device is normal.

- On the FTP server, the user name for a device to log in to the FTP server is admin, and the password is admin. The files to be downloaded are placed in the FTP server directory.
- The device acts as the FTP client to upload files to and download files from the FTP server.

### Network Topology



Figure4–1 Network Topology for Configuring a Device as an FTP Client

### Configuration Steps

- Step 1: Create Virtual Local Area Networks (VLANs), and add ports to the required VLANs. (Omitted)
- Step 2: Configure an FTP server, and place the files to be downloaded in the FTP server directory. (Omitted)
- Step 3: Configure the IP addresses of the devices so that the network between the client and the server is normal. (Omitted)
- Step 4: Device acts as the FTP client to upload files to and download files from the FTP server. (Omitted)

#In the file system mode of Device, copy one file from the FTP server to the file system of Device.

```
Device#filesystem
Device(config-fs)#copy ftp 2.0.0.1 admin admin sp4-g-6.5.0(41).pck file-system sp4-g-6.5.0(41).pck
Device (config-fs)#exit
```

#In the file system mode of Device, copy the startup file of Device into the FTP server.

```
Device#filesystem
Device(config-fs)#copy file-system startup ftp 2.0.0.1 admin admin startup.txt
```

- Step 5: Check the result.

#After the copy process is completed, check whether the downloaded file exists in the file system of Device.

In the FTP server, check whether the uploaded file exists. (Omitted)

```
Device(config-fs)#dir
size      date      time      name
-----
101526    MAR-01-2013 01:17:18  logging
10147     MAR-26-2013 07:58:50  startup
10207     MAR-01-2013 01:17:54  history
1372     MAR-23-2013 08:18:38  devInfo
```

6598624 MAR-26-2013 07:51:32 sp4-g-6.5.0(41).pck  
1024 JAN-10-2013 17:30:20 snmp <DIR>  
0 JAN-31-2013 14:29:50 syslog  
736512 MAR-27-2013 10:30:48 web-Spl-1.1.168.rom

---

## Note

- If the "FTP: Ctrl socket connect error(0x3c): Operation timed out" message is printed, it indicates that the server cannot be reached, and the cause may be that the route is not available or the server has not been started.
  - If the "Downloading##OK!" message is printed, it indicates that the file is copied successfully.
- 

### 4.3.2 Configure a Device as an FTP Server

#### Network Requirements

- Device1 acts as an FTP server, while PC and Device2 act as FTP clients. The network between the client and the server is normal.
- On the FTP server Device1, the user name is admin1, and the password is admin1. The file system directory of Device1 acts as the root directory of the FTP server.
- The PC and Device2 act as the FTP client to upload files to and download files from the FTP server Device1.

#### Network Topology

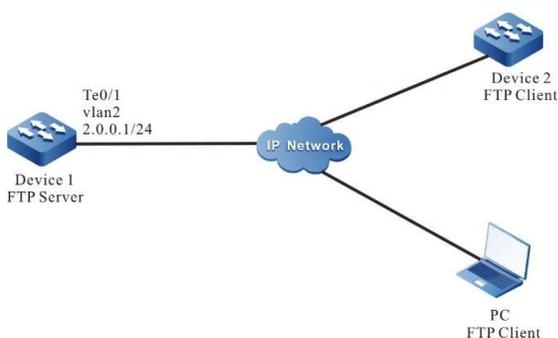


Figure4–2 Network Topology in Which a Device Acts as an FTP Server

#### Configuration Steps

- Step 1: Create Virtual Local Area Networks (VLANs), and add ports to the required VLANs.  
(Omitted)

Step 2: Configure the IP addresses of the interfaces so that the network between the PC, Device 2, and Device 1 are normal. (Omitted)

Step 3: On Device1, enable the FTP service, and configure the authorized user name and password.

#On Device1, enable the FTP service, and configure the authorized user name and password.

```
Device1#configure terminal
Device1(config)#local-user admin1 class manager
Device1(config-user-manager-admin1)#service-type ftp
Device1(config-user-manager-admin1)#password 0 admin1
Device1(config-user-manager-admin1)#exit
```

#On Device1, enable the FTP service.

```
Device1(config)#ftp enable
```

#On Device1, set the maximum number of concurrent users to 2.

```
Device1(config)#ftp max-user-num 2
```

Step 4: Check the result.

#Check whether the FTP service function is enabled on Device1.

```
Device#show ip sockets
Active Internet connections (including servers)
PCB Proto Recv-Q Send-Q Local Address Foreign Address (state)
-----
27cf8a4 TCP 0 0 0.0.0.0.80 0.0.0.0 LISTEN
27ce0a4 TCP 0 0 130.255.104.43.22 130.255.98.2.3590 ESTABLISHED
27d0be4 TCP 0 0 0.0.0.0.21 0.0.0.0 LISTEN
27d0824 TCP 0 0 127.0.0.1.2622 127.0.0.1.1026 ESTABLISHED
```

If the FTP service function has enabled, you can find that port 21 is in the listen state.

Step 5: Use Device2 as an FTP client to copy a startup file from FTP server Device1 to local.

```
Device2#filesystem
Device2(config-fs)#copy ftp 2.0.0.1 admin1 admin1 startup file-system startup
```

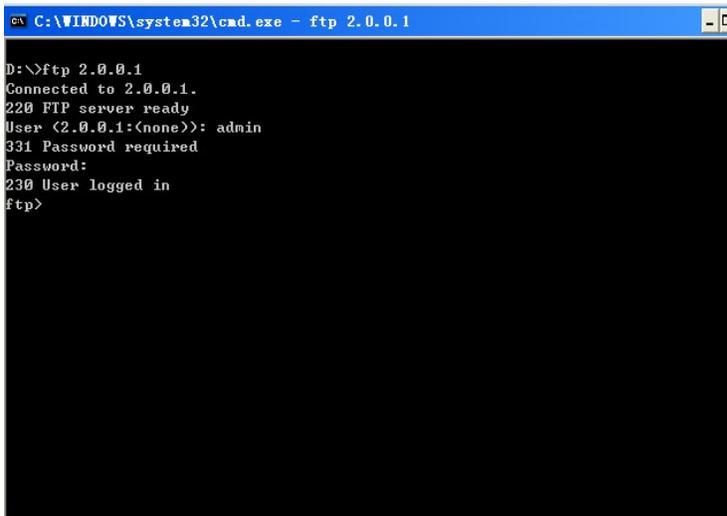
Step 6: Use PC as an FTP client to copy a startup file from FTP server Device1 to PC.

#In the following part, the Windows DOS screens are taken as an example to illustrate the process.

#In the Windows DOS screen, input the correct IP address, user name, and password to log in to the FTP server.

```
D:\>ftp 2.0.0.1
Connected to 2.0.0.1.
220 FTP server ready
User (2.0.0.1:(none)): admin
331 Password required
Password:
230 User logged in
```

ftp>

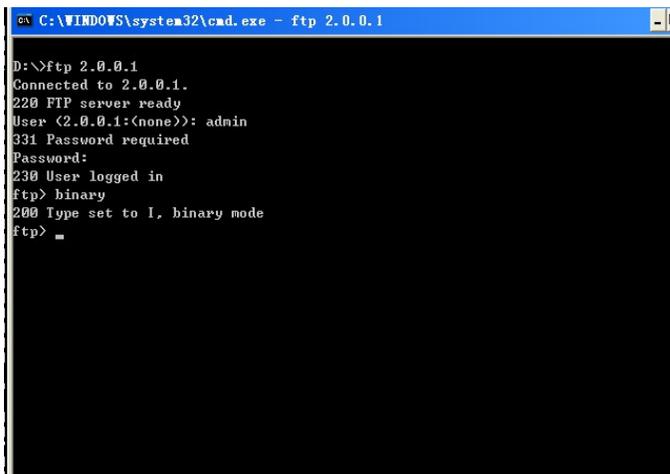


```
C:\WINDOWS\system32\cmd.exe - ftp 2.0.0.1
D:\>ftp 2.0.0.1
Connected to 2.0.0.1.
220 FTP server ready
User (2.0.0.1:(none)): admin
331 Password required
Password:
230 User logged in
ftp>
```

Figure 4–3 Logging in to the FTP server from the DOS interface

#Configure the PC and FTP server to transmit data in binary mode.

ftp>binary



```
C:\WINDOWS\system32\cmd.exe - ftp 2.0.0.1
D:\>ftp 2.0.0.1
Connected to 2.0.0.1.
220 FTP server ready
User (2.0.0.1:(none)): admin
331 Password required
Password:
230 User logged in
ftp> binary
200 Type set to I, binary mode
ftp>
```

Figure 4–4 Configuring the PC and FTP Server to Transmit data in Binary Mode

#Obtain the startup file in the file system of the FTP server Device1.

ftp>get startup

```
C:\WINDOWS\system32\cmd.exe - ftp 2.0.0.1
D:\>ftp 2.0.0.1
Connected to 2.0.0.1.
220 FTP server ready
User (2.0.0.1:(none)): admin
331 Password required
Password:
230 User logged in
ftp> binary
200 Type set to I, binary mode
ftp> get startup
200 Port set okay
150 Opening BINARY mode data connection
226 Transfer complete
ftp:Receive2758 bytes, cost 0.198seconds 14.75Kbytes/sec.
ftp> _
```

Figure4-5 Copying a Configuration File from the FTP Server

After the file copy process is completed, the file is available in the specified Windows directory.

---

 **Note**

- If the "421 Session limit reached, closing control connection" message is printed, it indicates that the number of connections has exceeds the maximum number allowed by the server.
- When you use a device to copy a file, if the " Ctrl socket connect error(0x3c): Operation timed out" message is printed, the cause may be that the server function is not enabled, or the route between the server and the client is not reachable.
- When you connect the FTP server through the FTP client PC, if the " connect :Unknown error number" is printed, the cause may be that the server function is not enabled, or the route between the server and the client is not reachable.

ssac modessac mode

---

### 4.3.3 Configure a Device as an TFTP Client

#### Network Requirements

- A PC acts as a TFTP server, and Device acts as a TFTP client. The network between the server and the device is normal. The files to be downloaded are placed in the TFTP server directory.
- The device acts as the TFTP client to upload files to and download files from the TFTP server.

#### Network Topology



Figure 4–6 Network Topology in Which a Device Acts as a TFTP Client

### Configuration Steps

- Step 1: Create Virtual Local Area Networks (VLANs), and add ports to the required VLANs. (Omitted)
- Step 2: Configure the IP addresses of all interfaces so that the network between the client and the server is normal. (Omitted)
- Step 3: Enable the TFTP server function on PC, and place the files to be downloaded in the TFTP server directory. (Omitted)
- Step 4: Device acts as the TFTP client to upload files to and download files from the TFTP server.

#On Device, copy a file from the TFTP server to the file system of Device.

```

Device#filesystem
Device(config-fs)#copy tftp 2.1.2.1 sp4-g-6.5.0(41).pck file-system sp4-g-6.5.0(41).pck
Device(config-fs)#exit
  
```

#On Device, copy the startup file from Device to the TFTP server.

```

Device#filesystem
Device(config-fs)#copy startup-config tftp 2.1.2.1 startup.txt
  
```

- Step 5: Check the result.

After the copy process is completed, check whether the downloaded file exists in the file system of Device. In the TFTP server, check whether the uploaded file exists. (Omitted)

```

Device(config-fs)#dir
size    date    time    name
-----  -
102227  MAR-01-2013  05:24:32  logging
10147   MAR-26-2013  07:58:50  startup
10202   MAR-01-2013  05:26:46  history
6598624 MAR-26-2013  07:51:32  sp4-g-6.5.0(41).pck
1024    JAN-10-2013  17:30:20  snmp      <DIR>
0       JAN-31-2013  14:29:50  syslog
736512  MAR-27-2013  10:30:48  web-Spl-1.1.168.rom
  
```



- 
- If the "Downloading#####OK!" message is printed, it indicates that the file copy is successful. The message shows the file size, which is determined by the actual file size.
  - When you use a device to copy a file, if the "tftp Failed! ErrorNum: 0x41, ErrorType: Host unreachable." message is printed, the cause may be that the TFTP server function is not enabled, or the route between the server and the client is not reachable.
- 

### 4.3.4 Configure a Device as an SFTP Client

#### Network Requirements

- Take the PC as an SFTP server, and the device acts as an SFTP client. The network between the server and the device is normal.
- On the SFTP server, the user name for a device to log in to the SFTP server is admin, and the password is admin. The files to be downloaded are placed in the SFTP server directory.
- The device acts as the SFTP client to upload files to and download files from the SFTP server.

#### Network Topology



Figure4–7 Network Topology for Configuring a Device as an SFTP Client

#### Configuration Steps

- Step 1: Configure an SFTP server, and place the files to be downloaded in the SFTP server directory. (Omitted)
- Step 2: Configure the IP addresses of the devices so that the network between the client and the server is normal. (Omitted)
- Step 3: Device acts as the SFTP client to upload files to and download files from the SFTP server.

#Download a file from the SFTP server to the file system of the device.

```
Device#sftp get 2.0.0.1 22 admin admin sp8-g-6.6.7(46)-dbg.pck sp8-g-6.6.7(46)-dbg.pck
The authenticity of host '2.0.0.1 (2.0.0.1)' can't be established.
RSA key fingerprint is e4:dd:11:2e:82:34:ab:62:59:1c:c8:62:1d:4b:48:99.
Are you sure you want to continue connecting (yes/no)? yes

Downloading#####
#####
```

#Upload the startup file in the file system of Device to the SFTP server.

```

Device#sftp put 2.0.0.1 22 admin admin startup startup.txt
The authenticity of host '2.0.0.1 (2.0.0.1)' can't be established.
RSA key fingerprint is e4:dd:11:2e:82:34:ab:62:59:1c:c8:62:1d:4b:48:99.
Are you sure you want to continue connecting (yes/no)? yes
Uploading#####
#####

```

Step 4: Check the result.

#After the copy process is completed, check whether the downloaded file exists in the file system of the device. In the SFTP server, check whether the uploaded file exists. (Omitted)

```

Device(config-fs)#dir
size    date    time    name
-----  -
101526  MAR-01-2015  01:17:18  logging
10147   MAR-26-2015  07:58:50  startup
10207   MAR-01-2015  01:17:54  history
11676148  MAR-26-2013  07:51:32  sp8-g-6.6.7(46)-dbg.pck
2048    JAN-10-2015  17:30:20  snmp      <DIR>

```

### 4.3.5 Configure a Device as an SFTP Server

#### Network Requirements

- Device acts as an SFTP server, while a PC acts as an SFTP client. The network between the client and the server is normal.
- On the SFTP server Device, the user name is admin1, and the password is admin1. The file system directory of Device acts as the root directory of the SFTP server.
- A PC acts as the SFTP client to upload files to and download files from the SFTP server Device.

#### Network Topology



Figure 4–8 Network Topology for Configuring a Device as an SFTP Server

#### Configuration Steps

Step 1: Configure IP addresses for the ports so that the network between the PC and the device is normal. (Omitted)

Step 2: On Device, enable the SFTP service, and configure the authorized user name and password.

#On the SFTP server Device, configure the authorized user name and password.

```

Device#configure terminal
Device(config)#local-user admin1 class manager
Device(config-user-manager-admin1)#service-type ssh
Device(config-user-manager-admin1)#password 0 admin1

```

```
Device(config-user-manager-admin1)#exit
```

#Enable SSH service on Device (SFTP is a sub-module of the SSH protocol)

```
Device(config)#ip ssh server
```

Step 3: The PC acts as the SFTP client to upload files to and download files from the SFTP server Device.

#In the following part, the Linux system is taken as an example to illustrate the process.

#Input the correct IP address, user name, and password to log in to the SFTP server.

```
[root@aas ~]# sftp admin1@2.1.1.1
Connecting to 2.1.1.1...
admin1@2.1.1.1's password:
sftp>
```

#Obtain the startup file in the file system of the SFTP server Device.

```
sftp> get startup startup
Fetching /flash/startup to startup
/flash/startup                               100% 13KB 12.9KB/s 00:00
```

#After the file copy process is completed, the file is available in the specified operation directory.

```
sftp> ls
sp8-g-6.6.7(74)-dbg.pck  sp8-g-6.6.7(76)-dbg.pck  startup          tech          test_pc
sftp>
```

#Upload the files in the PC to the file system of SFTP server Device.

```
sftp> put sp8-g-6.6.7(76)-dbg.pck sp8-g-6.6.7(76)-dbg.pck
Uploading sp8-g-6.6.7(76)-dbg.pck to /flash/ sp8-g-6.6.7(76)-dbg.pck
sp8-g-6.6.7(76)-dbg.pck                       100% 11424KB 16.0KB/s 00:00
```

#After the file copy process is completed, the file is available in the file system of the device.

```
Device(config-fs)#dir
size      date      time      name
-----
2048      JUN-30-2015 16:35:50 tech      <DIR>
10229     JUN-12-2015 14:31:22 history
101890    JUN-30-2015 17:46:40 logging
39755     JUN-30-2015 16:33:56 startup
740574    MAY-27-2014 18:55:14 web-Spl-1.1.243.rom
2048      JUN-27-2015 16:26:10 snmp      <DIR>
11698172  JUN-30-2015 10:36:18 sp8-g-6.6.7(76)-dbg.pck
```

### 4.3.6 Configure a Device as an FTPS Client

#### Network Requirements

- A PC acts as an FTP server, and the device Device acts as an FTP client. The network between the server and the device is normal.

- Secure data transmission is guaranteed by establishing secure data channels between the FTP Server and the FTP Client.
- FTP client can upload files to and download files from the FTP server.

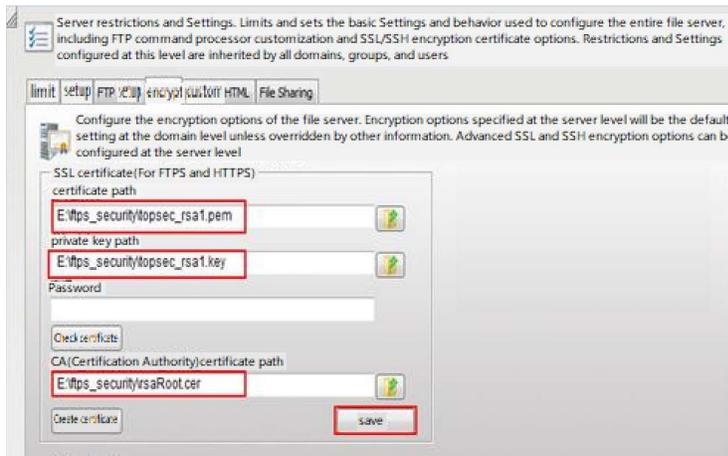
## Network Topology



Figure 4–9 Network Topology for Configuring a Device as an FTPS Client

## Configuration Steps

- Step 1: Configure IPv4 addresses for the ports. (Omitted)
- Step 2: Install certificate on FTP Server and set FTP user certificate path, private key path, and CA certificate path.



- Step 3: FTP Client imports FTP CA certificate, user certificate, and private key.

#Create a domain test on the device:

```

Device#configure terminal
Device(config)#crypto ca identity test
Device(ca-identity)#exit
  
```

#ftp binds to domain test:

```

Device(config)#ip ftp secure-identity test
  
```

#Open the CA certificate (rsaRoot.cer) in Notepad, then copy the content, type crypto ca import certificate to test in shell, and follow the prompts to import the certificate into the device domain test:

```

Device(config)#crypto ca import certificate to test
  
```



```

MIICXQIBAABKgQDoCU2pOc2xX1jKKPa1MymkH0LIUIu2Q+H0qUir9IOVWGskQP43kdV9BDJlhL/PglYCKnnR3I/X40/
5u8/6lv0J8Ronz45thCd9QfqqI9xwuRY7ddhqe7oPdkQwlic3CCVlqaTU9xz6P7LNaFbgwMVxtKxD7wnlTOV6wWFTsaddpw
IDAQABAoGBAMnJNWliJFgI4+1CvHGN4buhmApWBnnmBL1A7jrlh4CMGPI5MJrgzvjEsnlwfWIXJXbSu4feuJT1UFqMk
uyIm9l+k8Rm3hjCIXIIfNV/ykG6a6GIVFYGxQWhaL50Pm6S7xXL9Ryd6hnOHUUtwtuLvkpBTx/4qvrIABDtXRjVglvApAk
EA9BN1ZxM31BOyeB6KXvvmXD6/+dGaDfE4Dbcijy1LgKliaEBJ00e/0R9ekg6myGTU2asJvPtkaXPqcvwU6+e2mwJBAPN
fRtk9LzUINmTV2DrsE9k3rbPnqqS9wb/mLUNdv2FQeoY/Zf4qh0WXsug2q/6GpsvLUA7mbdArGFUwwQbw3+UCQQC8r2
5LSOgX40JM6g8+bq4fEcOHdSoLLTeQIststC9yP3/75/cqhoUbPYz2jK0SriB+RWM53X46p4nPdo4b8P2RAkBGjoBLL+nXx
ooWgcjGjFrUxsedOLTIPhtFvz2wliWx2NsswISZQ0skae58VB1ZFSJvguoa58M+bsAHMrNDh+HhAkBcNAjKBDdVw0l16bN
oRGugEvu03Z3O0kbVcjZld+4aVG4DzvEp1ZbsYRv9YPMtpnzmB7WZUshAL99nHnHxtbh
-----END RSA PRIVATE KEY-----

```

```

Nov 11 2015 19:06:56: %PKI-CERTIFICATE_STATECHG-5: Certificate(issuer:C=CN, ST=BEIJING, O=CIECC, OU=GFA
CA, CN=MiniCA FreeBSD Root Cert, sn:109EEDC1B977A43973273F7D0C538A3B, subject:C=CN, ST=beijing,
L=dongcheng, O=ciecc, OU=gfa, E=test@ec.com.cn, CN=rsa2) state valid
% PKI: Import Certificate success.

```

#After the certificate is successfully imported, you can view the status as Valid using the show crypto ca certificates command:

```

Device#show crypto ca certificates
Root CA Certificate:
  Status: Valid
  Serial Number: 4e95e7d7b1e3fc0b
  Subject: C=CN, ST=BEIJING, O=CIECC, OU=GFA CA, CN=MiniCA FreeBSD Root Cert
  Issuer : C=CN, ST=BEIJING, O=CIECC, OU=GFA CA, CN=MiniCA FreeBSD Root Cert
  Validity
    Start date: 2009-08-03 06:06:52
    End date: 2019-08-03 06:06:52
  Key Type: RSA(1023 bit)
  Usage: General
  Fingerprint(sm3):18d39e4c50c9ad8b11446ac7ac1736f853ac92e769994b98233b48787562429c
  Fingerprint(sha1):ab3559e26384539ffcac3c76b5a5e7a1f7073dfb
  Associated Identity: test
    index: 3

My Certificate:
  Status: Valid
  Serial Number: 109eedc1b977a43973273f7d0c538a3b
  Subject: C=CN, ST=beijing, L=dongcheng, O=ciecc, OU=gfa, E=test@ec.com.cn, CN=rsa2
  Issuer : C=CN, ST=BEIJING, O=CIECC, OU=GFA CA, CN=MiniCA FreeBSD Root Cert
  Validity
    Start date: 2012-06-26 05:01:23
    End date: 2032-06-26 05:01:23
  Key Type: RSA(1024 bit)
  Usage: General
  Fingerprint(sm3):504599a2f170c51b62b2f8b0850f33a5595bc9e592d14cae9e90b1e59de35a89
  Fingerprint(sha1):080614a82cc4f3786458c585f9a58edf19da19bd
  Associated Identity: test
    index: 4

```

Step 4: FTP client uploads files to and downloads files from the FTP server.

FTP client uploads files to the FTP server:

```

Device#filesystem
Device1(config-fs)#copy file-system startup ftps 2.0.0.1 a a startup VerifyType peer

Copying!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Total 103440 bytes copying completed.

```

FTP client downloads files from the FTP server:

```

Device(config-fs)#ftpscopy 2.0.0.1 a a test.doc test.doc VerifyType peer

Downloading#####
#####

```

##### OK!

Step 5: Check the result.

#After the file download process is completed, view the file in the file system of Device.

```
Device(config-fs)#dir
  size   date      time    name
-----
10189   NOV-04-2015 20:27:03 history
436578  NOV-04-2015 20:33:08 test.doc
```

# 5 File System Management

---

## 5.1 Overview

The following lists the storage medium of the device and their functions:

- SDRAM: Synchronous Dynamic Random Access Memory (SDRAM) provides the space for executing application programs of the device.
- FLASH: Stores application programs, configuration files, and the BootROM programs, and so on.
- EEPROM: Electrically Erasable and Programmable Read-Only Memory, stores system configuration files and user information which is frequently changed.
- USB: Used to store user data.

The device manages the following types of files:

- BootROM files: Store basic data for system initialization.
- Device application programs: Implement tasks such as route forwarding, file management, and system management.
- Configuration files: Store the system parameters that are configured by the users.
- Log files: Stores system log information.

---

### Note

- The filesystem command is used to access the file system and can be run on both Master and Slave.
- 

## 5.2 File System Management Function Configuration

Table 5-1 File System Management Function Configuration List

Configuration Task	
Manage storage devices.	Display the information about a storage device.
	Format a storage device.
Manage file directories.	Display the information about a file directory.
	Display the current working path.
	Change the current working path.
	Create a directory.
	Delete a directory.
Manage file operations	Copy a file.
	Rename a file.
	Display the content of a file.
	Delete a file.
Execute a configuration file manually.	Execute a configuration file manually.
Configure startup parameters.	Configure startup parameters.

### 5.2.1 Manage storage devices.

#### Configuration Condition

Before performing operations on storage devices, ensure that:

- The system has started normally.

#### Display the information about a storage device.

By displaying the information about a storage device, you can view the features of the storage device and the size of the remaining space.

Table 5-2 Displaying the Information about a Storage Device

Step	Command	Description
Enter the file system configuration mode.	<b>filesystem</b>	-
Display the information about a storage device.	<b>volume</b>	Mandatory

### Format a storage device.

If the space of a storage device is unavailable, you can use the format command to format the storage device.

Table 5-3 Formatting a Storage Device

Step	Command	Description
Enter the file system configuration mode.	<b>filesystem</b>	-
Format a storage device.	<b>format { /flash   /syslog   /usb }</b>	Optional

---

## Caution

- Exercise caution in formatting a storage device, because the operation may cause permanent loss of all files on the storage device, and the files cannot be recovered.
- 

## 5.2.2 Manage file directories.

### Configuration Condition

Before performing operations on file directories, ensure that:

- The system has started normally.

### Display the information about a file directory.

By displaying the information about a file directory, you can view the details of the files in the specified directory.

Table 5-4 Displaying File Directory Information

Step	Command	Description
Enter the file system configuration mode.	<b>filesystem</b>	-
Display the information about a directory.	<b>dir</b> [ <i>path</i> ]	Mandatory

**Display the current working path.**

By displaying the current working path, you can view the details of the current path.

Table 5-5 Displaying the Current Working Path

Step	Command	Description
Enter the file system configuration mode.	<b>filesystem</b>	-
Display the current working path.	<b>pwd</b>	Mandatory

**Change the current working path.**

By changing the current working path, you can switch over a user to the specified directory.

Table 5-6 Changing the Current Working Path

Step	Command	Description
Enter the file system configuration mode.	<b>filesystem</b>	-
Change the current working path.	<b>cd</b> <i>path</i>	Mandatory

**Create a directory.**

If you want to create a directory in the file system, perform this operation.

Table 5-7 Creating a Directory

Step	Command	Description
Enter the file system configuration mode.	<b>filesystem</b>	-
Create a directory.	<b>mkdir</b> <i>directory</i>	Mandatory

### Delete a directory.

If you delete a directory through this operation, all sub-directories and files in the directory are deleted.

Table 5-8 Deleting a Directory

Step	Command	Description
Enter the file system configuration mode.	<b>filesystem</b>	-
Delete a directory.	<b>rmdir</b> <i>directory</i> [ <b>force</b> ]	Mandatory

---

### Note

- Exercise caution when deleting a directory, because the operation of deleting the directory may permanently delete all sub-directories and files in the directory, and the files cannot be recovered.
- 

## 5.2.3 Manage file operations

### Configuration Condition

Before performing operations on files, ensure that:

- The system has started normally.

### Copy a file.

In the file system, you can copy a file to the specified directory.

Table 5-9 Copying a File

Step	Command	Description
Enter the file system configuration mode.	<b>filesystem</b>	-
Copy a file.	<b>copy</b> <i>src-parameter dest-parameter</i>	Mandatory

## Note

- The copy command can be used to copy files between the file system, the FTP server, and the TFTP server. For details, refer to the section on the usage of the copy command in the configuration manual.

### Rename a file.

In the file system, you can change the name of a file into a specified name.

Table 5-10 Renaming a File

Step	Command	Description
Enter the file system configuration mode.	<b>filesystem</b>	-
Rename a file.	<b>rename</b> <i>src-filename dest-filename</i>	Mandatory

### Display the content of a file.

In the file system, you can view the content of a file.

Table 5-11 Displaying the Content of a File

Step	Command	Description
Enter the file system configuration mode.	<b>filesystem</b>	-
Display the content of a file.	<b>type</b> <i>path/filename</i>	Mandatory

## Delete a file.

In the file system, you can delete a file that is no longer in need.

Table 5-12 Deleting a File

Step	Command	Description
Enter the file system configuration mode.	<b>filesystem</b>	-
Delete a file.	<b>delete <i>path/filename</i></b>	Mandatory

---

### Note

- Exercise caution when you use the delete command because it permanently deletes a file, and the file cannot be recovered.
- 

## 5.2.4 Download a File from FTP

### Configuration Condition

Before manually downloading the file from the FTP, first complete the following tasks:

- The system has started normally.
- Ensure that the route between the FTP server and the device interface is reachable and the route can be pinged through.

### Download a File from the FTP Server

Use a command for downloading the file from the FTP and you can download the related file on the FTP server to the file system

Table 5-13 Downloading a File from the FTP server

Step	Command	Description
Enter the file system configuration mode.	<b>filesystem</b>	-

Step	Command	Description
Download a File from the FTP Server	<pre> <b>ftpcopy</b> [ <b>vrf</b> <i>vrf-name</i> ] <i>host-ip-address</i> <i>username</i> <i>password</i> <i>src-filename</i> { <b>/flash</b>   <b>/syslog</b>   <b>/usb</b>   <i>dest-filename</i> }  <b>ftpscopy</b> [ <b>vrf</b> <i>vrf-name</i> ] <i>host-ip-address</i> <i>username</i> <i>password</i> <i>src-filename</i> { <b>/flash</b>   <b>/syslog</b>   <b>/usb</b>   <i>dest-filename</i> } <b>VerifyType</b> { <b>none</b>   <b>peer</b> } </pre>	Optional

---

## Note

- The ftpcopy command can be used to download files from the FTP server to the file system. For details, refer to the section on the usage of the ftpcopy command and the ftpscopy command in the configuration manual.
- 

## 5.2.5 Configure startup parameters.

### Configuration Condition

Before configuring startup parameters, ensure that:

- The system has started normally.

### Configure startup parameters.

\In configuring startup parameters, you can configure the application program file that is to be used in the next startup.

Table 5-14 Configuring Startup Parameters

Step	Command	Description
Enter the file system configuration mode.	<b>filesystem</b>	-

Step	Command	Description
Configure startup parameters.	<b>boot-loader</b> <i>path/filename</i> [ <i>bootline-number</i> ]	Mandatory

## 5.2.6 File System Managing, Monitoring, and Maintaining

Table 5-15 File System Managing, Monitoring, and Maintaining

Command	Description
<b>clear boot-loader</b> [ <i>bootline-number</i> ]	Clear the startup parameters with the specified index.
<b>show filesystem</b>	Display the information about the file system.
<b>show file location</b>	Display the location of the system file in the file system.
<b>show file descriptor</b>	Display the location of the system file in the file system and the descriptor.
<b>show boot-loader</b>	Display the system startup parameters.

## 5.3 Typical Configuration Example of File System Management

### 5.3.1 Configure startup parameters.

#### Network Requirements

None

#### Network Topology

None

#### Configuration Steps

Step 1: Enter the file system configuration mode.

Step 2: Configure system startup options.

#View the system startup parameters.

```
Device#filesystem
Device(config-fs)#show boot-loader
The app to boot at the next time is: flash0: /flash/sp26-g-9.5.0.2(20)(R).pck
The app to boot at the this time is: flash0: /flash/sp26-g-9.5.0.2(20)(R).pck
Boot-loader0: flash0: /flash/sp26-g-9.5.0.2(20)(R).pck

Device(config-fs)#exit
```

**#Copy the file sp26-g-9.5.0.2(20)(R).pck to flash via ftp, and then modify the sp26-g-9.5.0.2(20)(R).pck file in flash to be the next system startup option, and set the priority to 0.**

```
Device#filesystem
Device(config-fs)#boot-loader /flash/sp26-g-9.5.0.2(20)(R).pck

Boot-loader0 set OK
Device(config-fs)#exit
```

**#View the configuraiton result.**

```
Device(config-fs)#show boot-loader
The app to boot at the next time is: flash0: /flash/sp26-g-9.5.0.2(20)(R).pck
The app to boot at the this time is: flash0: /flash/sp26-g-9.5.0.2(20)(R).pck

Boot-loader0: flash0: /flash/sp26-g-9.5.0.2(20)(R).pck
Boot-loader4: backup0: sp26-g-9.5.0.2(20)(R).pck
Device(config-fs)#exit
```

# 6 Configuration File Management

---

## 6.1 Overview

Configuration file management is a function that is used to manage device configuration files. Through the command line interface provided by the device, users can easily manage configuration files. If the device needs to automatically load the current configuration of users after restart, the current configuration commands must be saved into the configuration file before the device restarts. Users can upload configuration files to or download configuration files from another device through FTP or TFTP, realizing batch device configuration. The device configuration is categorized into the following two types:

Startup configuration:

When the device starts, it loads the startup configuration file with the name "startup" by default, and it completes the initialization configuration of the device. This configuration is called startup configuration. Here the device has two startup configuration files, one is the default startup configuration file, and the other is the backup startup configuration file. When the device starts, if the default startup configuration file does not exist, the system copies the backup startup configuration file to the location of the default startup configuration file and loads this startup configuration file.

Current configuration:

Current configuration is a set of commands that take effect currently. It consists of startup configuration and the configuration that is added or modified by the user after startup. The current configuration is saved in the memory database. If the current configuration is not saved into the startup configuration file, the configuration information gets lost after the device restarts.

The following describes the contents and formats of the configuration files:

- Configuration files are saved in the file system in the form of text files.
- The contents of the configuration files are saved in the form of configuration commands, and only non-default configuration is saved.
- Configuration files are organized based on command modes. All commands in one command mode are organized together to form a paragraph.
- Paragraphs are organized according to a certain rule: system configuration mode, interface configuration mode, and configuration modes of different protocols.

- Commands are organized according to their relations. The related commands form a group, and different groups are separated by blank lines.

## 6.2 Configuration File Management Function Configuration

Table 6-1 Configure File Management List

Configuration Task	
Save the current configuration.	Save the current configuration.
Back up device configuration.	Back up the current configuration.
	Back up the startup configuration.
Restore the startup configuration.	Restore the startup configuration.

### 6.2.1 Save the current configuration.

#### Configuration Condition

None

#### Save the current configuration.

If the current configuration of the user can take effect only after the device starts, you need to save the current configuration into the startup configuration file.

Table 6-2 Saving the Current Configuration

Step	Command	Description
Save the current configuration to the startup configuration file.	<b>write</b>	Mandatory

#### Note

- If the device is restarted or powered off while the configuration file is being saved, configuration information may get lost.
- Saving the current configuration not only saves the configuration to the startup

---

configuration file, but also saves the configuration to the backup startup configuration file.

---

## 6.2.2 Configure the Backup System

### Configuration Condition

Before configuring the backup system parameters, ensure that:

- The route between the device and the server is reachable.
- The configuration file to be backed up exists; otherwise, backup fails.

### Back up the current configuration.

In backing up the current configuration, you can use a command to back up the current configuration to the FTP server.

Table 6-3 Backing Up the Current Configuration

Step	Command	Description
Enter the file system configuration mode.	<b>filesystem</b>	-
Back up the current configuration to a remote host through the FTP protocol.	<b>copy running-config { file-system dest-filename   ftp [ vrf vrf-name ] { hostname   ip-address } username password dest-filename   startup-config   tftp [ vrf vrf-name ] { hostname   ip-address } dest-filename ftps [ vrf vrf-name ] { hostname   ip-address } username password dest-filename VerifyType { none   peer } }</b>	Mandatory

### Back up the startup configuration.

In backing up the startup configuration, you can use a command to back up the startup configuration to the FTP server.

Table 6-4 Backing Up the Startup Configuration

Step	Command	Description
Enter the file system configuration mode.	<b>enable</b>	-
Save the startup configuration to a remote host through the FTP protocol.	<b>copy startup-config { file-system dest-filename   ftp [ vrf vrf-name ] { hostname   ip-address } username password dest-filename   ftps [ vrf vrf-name ] { hostname   ip-address } username password dest-filename VerifyType { none   peer }   tftp [ vrf vrf-name ] { hostname   ip-address } dest-filename }</b>	Mandatory

### 6.2.3 Restore the startup configuration.

#### Configuration Condition

Before restoring the startup configuration, ensure that:

- The route between the device and the server is reachable.
- The configuration file that is to be restored exists.

#### Restore the startup configuration.

In restoring the startup configuration, you can use a command to download the startup configuration file from the FTP server and set it as the startup configuration file that is used after restart. In this way, after the device is restarted, the device can load the startup configuration file.

Table 6-5 Restoring the Startup Configuration

Step	Command	Description
Enter the file system configuration mode.	<b>filesystem</b>	-
Restore the startup configuration.	<b>copy { file-system src-filename   ftp [ vrf vrf-name ] { hostname   ip-address } username password src-filename   ftps [ vrf vrf-name ] { hostname   ip-address } username password src-</b>	Mandatory

Step	Command	Description
	<i>filename</i>   <b>tftp</b> [ <b>vrf vrf-name</b> ] { <i>hostname</i>   <i>ip-address</i> } <i>src-</i> <i>filename</i> } { <b>file-system dest-</b> <i>filename</i>   <b>startup-config</b> }	

## Note

- Before overwriting the local startup configuration, ensure that the configuration file matches the device type and matches the current system version.
- After performing the operation of restoring the startup configuration, the current configuration is not changed. After the device is restarted, the startup configuration is restored.

## 6.2.4 Configuration File Managing, Monitoring, and Maintaining

Table 6-6 Configuring File Management, Monitoring and Maintaining

Command	Description
<b>show running-config</b> [ <b>after-interface</b>   <b>before-interface</b>   <b>interface</b> [ <i>interface-name</i> ]   [ <i>configuration</i> ] ] [ { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>expression</i>   <b>redirect</b> { <b>file</b> <i>file-name</i>   <b>ftp</b> [ <b>vrf vrf-name</b> ] { <i>hostname</i>   <i>ip-address</i> } <i>user-name password file-name</i> } }   <b>ftps</b> [ <b>vrf vrf-name</b> ] { <i>hostname</i>   <i>ip-address</i> } <i>user-name password file-name</i> } } ]	Display the current configuration information.
<b>show startup-config</b> [ <i>file-number</i>   {   { <b>begin</b>   <b>exclude</b>   <b>include</b> [ <b>context</b> ] } <i>expression</i>   <b>redirect</b> { <b>file</b> <i>filename</i>   <b>ftp</b> { [ <b>vrf vrf-name</b> ] { <i>hostname</i>   <i>ip-address</i> } <i>user-name password file-name</i> } }   <b>ftps</b> { [ <b>vrf vrf-name</b> ] { <i>hostname</i>   <i>ip-address</i> } <i>user-name password file-name</i> } } } ]	Display the startup configuration information.

## 6.2.5 Configuration File Encryption

### Configuration Condition

- Configuration file encryption requires a USB device to be plugged in.

### Configure Encryption of Configuration Files

Configuration file encryption is to encrypt the configuration file using the SM4 algorithm, the key is specified by the user, when the user specifies the key, it will encrypt the configuration file when the next write action is executed.

Operation record encryption refers to encrypting the configuration file using the State Secrets SM4 algorithm, the key is specified by the user, and when the user specifies the key, the encryption starts for the subsequent operation records.

Table 6-7 Configuration File Encryption and Operation Record Encryption

Step	Command	Description
Enter the global configuration mode.	<b>config terminal</b>	-
Configuration File Encryption	<b>service encryption startup algorithms SM4 key</b> <i>password</i>	Configuration file encryption, and the user specifies the key.
Operation record encryption	<b>service encryption history algorithms SM4 key</b> <i>password</i>	Operation record encryption, and the user specifies the key.

---

### Note

- Encryption of the configuration file takes effect at the next write action executed after the encryption function is configured. Encryption of operation record takes effect immediately after the encryption function is configured.
  - An external USB device must be plugged in to configure the encryption function. The operation record encryption function does not require a USB device.
-

# 7 System Management

---

## 7.1 Overview

Through system management, users can view the current working status of the system, configure the basic functional parameters of the device, and perform basic maintenance and management of the device. System management provides the following functions: configure the device name, configure the system time and time zone, configure the login welcome message, configure the system exception processing mode, configure to restart the device, configure the password encryption service, configure the history command saving function, configure the login security service, configure monitor CPU, configure display of properties in pages.

## 7.2 System Management Function Configuration

Table 7-1 System Management Function Configuration List

Configuration Task	
Configure the device name.	Configure the device name.
Configure the system time and time zone.	Configure the system time and time zone.
Configure the login welcome message.	Configure the login welcome message.
Configure the system exception processing mode.	Configure the system exception processing mode.
Configure to restart the device.	Configure to restart the device.
Configure the encryption service.	Configure the encryption service.
Configure the history command saving function.	Configure the history command saving function.
Configure the login security service.	Configure the login security service.
Configure CPU monitoring.	Configure CPU monitoring.

Configuration Task	
Configure display of properties in pages.	Configure display of properties in pages.
Configure system security mode.	Configure system security mode.

### 7.2.1 Configure the device name.

#### Configuration Condition

None

#### Configure the device name.

A device name is used to identify a device. A user can change the device name according to the actual requirement. The modification takes effect immediately, that is, the new device name is displayed in the next system prompt.

Table 7-2 Configure the Device Name

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the device name.	<b>hostname</b> <i>host-name</i>	Mandatory

### 7.2.2 Configure the system time and time zone.

#### Configuration Condition

None

#### Configure the system time and time zone.

The system time and time zone is the time displayed in the timestamp of system information. The time is determined by the configured time and time zone. You can run the **show clock** command to view the time information of the system. To make the device work normally with other devices, the system time and time zone must be accurate.

Table 7-3 Configuring the System Time and Time Zone



When a system exception occurs, the system directly restarts to restore the system. The system exception processing mode is configured in three aspects: The first is enabling periodical exception detection. The system periodically detects the task status, code segment, and semaphore dead lock with a cycle of 10s, 10s, and 30s respectively. Secondly, an exception level is configured. If exceptions of the level and higher levels occur, the device restarts. Exception levels include: alert, critical, emergency, error, and warn. You can also configure the health monitoring exception processing mode, which includes the ignore mode and the reload mode.

Table 7-5 Configuring the System Exception Processing Mode

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure exception processing mode.	<b>exception { period-detect enable   reboot [ level { alert   critical   emergency   error   warn } ]   detect-health {ignore   reload} }</b>	Mandatory By default, Periodic exception detection is enabled, When an exception occurs, the exception level for device restart is <b>critical</b> ; By default, the health monitoring is enabled, and the processing mode by default is Ignore when an exception is detected by health monitoring.
Configure exception processing mode in stacking mode.	<b>exception { period-detect enable   reboot {device <i>device-num</i>   level device <i>device-num</i> { alert   critical   emergency   error   warn } }   detect-health <i>device-num</i> {ignore   reload} }</b>	Mandatory By default, Periodic exception detection is enabled, When an exception occurs, the exception level for device restart is <b>critical</b> ; By default, the health monitoring is enabled, and the processing mode by default is Ignore when

Step	Command	Description
		an exception is detected by health monitoring.

---

### Note

- If the device is configured to restart at a certain exception level, then an exception of the level and above occurs, the device will restart.
  - The exception levels in descending order are: emergency, alert, critical, error and warn.
- 

## 7.2.5 Configure to restart the device.

### Configuration Condition

None

### Restart a Device

When a device fault occurs, you can choose to restart the device according to the actual situation so as to eliminate the fault. The device restart modes include cold restart and hot restart. In a cold restart, the user can directly power off the device and power on the device again. In a hot restart, the user restarts the device by using a restart command. During the hot restart process, the device is not powered off.

Table 7-6 Restarting a Device

Step	Command	Description
Restart a device using the command or restart all active virtual switch member devices in the stacking domain using the command in stacking mode.	<b>reload</b>	Mandatory

---

### Note

- If you forcibly power off and restart a device that is in the operating status, hardware damage or data loss may be caused. Therefore, this restart mode is usually not
-

---

recommended.

- If you use the reload command to restart the device, all the services of the device are interrupted. Exercise caution when performing this operation.
- 

## 7.2.6 Configure the history command saving function.

### Configuration Condition

None

### Configure the history command saving function.

With the history command saving function, you can query and collect the history commands that have been executed. Before the history command saving function is configured, history commands are saved in the memory file system. After the function is configured, the system automatically saves history commands in the flash file system.

Table 7-7 Configuring the History Command Saving Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure to save history commands.	<b>shell-history save</b>	Mandatory By default, the history command saving function is enabled.

## 7.2.7 Configure the login security service.

### Configuration Condition

None

### Enable the System Login Security Service

To enhance the system security, the device provides the system login security service function. The functions include:

- Prevents brute force cracking of user login passwords.
- Prevents the fast connection function.

The function of brute force cracking prevention prevents malicious illegal users from forcedly cracking the user name and password for logging in to the device. If the system finds that the number of continuous login authentication failures of a user reaches the number specified by the system, the system rejects the login request from the IP address within the specified period of time.

The function of preventing fast connections prevents illegal users from initiating a large number of login requests within a short period time because this may occupy a lot of system and network resources. If the number of repeated login connections from a user reached a specified number, the system rejects the login connection requests from the IP address within the specified period of time.

Table 7-8 Enabling the System Login Security Service

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable the system login security service.	<b>service login-secure</b> <b>{ telnet   ssh   ftp   snmp }</b>	Mandatory By default, the system login security service is disabled.

### Configure the Parameters of the System Login Security Service

Table 7-9 Configuring the Parameters of the System Login Security Service

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the duration for Telnet module to forbid logins from an offending IP address.	<b>login-secure</b> telnet ip-addr <b>forbid-time</b> <i>forbid-time-number</i>	Mandatory By default, the duration is 10 minutes.
Configure the maximum number of continuous login authentication failures of an offending IP address forbidden by the Telnet module.	<b>login-secure</b> telnet ip-addr <b>max-try-time</b> <i>max-try-time-number</i>	Mandatory By default, the number is 5.
Configure the aging time for the Telnet module to forbid an offending IP	<b>login-secure</b> telnet ip-addr <b>record-aging-time</b> <i>record-aging-time-number</i>	Mandatory By default, the aging time is 15 minutes.

Step	Command	Description
address from recording information.		

## 7.2.8 Configure CPU monitoring.

### Configuration Condition

None

### Configure CPU monitoring.

Through CPU monitoring, the system monitors the CPU occupancy to learn the current operation status of the CPU. The following shows the contents of CPU monitoring:

- Monitor the CPU occupancy of each process in the system, and you can view the relevant information after configuration by entering the **show cpu** command. Enable the CPU occupancy history statistics function, and you can view the relevant information after configuration by using the **show cpu monitor** command.

Table 10-11 Configuring CPU Monitoring

Step	Command	Description
Enter the global configuration mode.	<b>enable</b>	-
Enable monitoring of CPU occupancy of each process.	<b>spy cpu</b>	Mandatory By default, the CPU occupancy monitoring function is not enabled.
Enable the CPU occupancy historical statistics function.	<b>monitor cpu</b>	Mandatory By default, the CPU occupancy historical statistics function is enabled.

## 7.2.9 Configure display of properties in pages.

### Configuration Condition

None

### Configure Display of Properties in Pages

System information can be displayed in pages, making it easy for users to view the information. Users can set to display device information in pages according to the actual requirement.

Table 7-12 Configuring Display of Properties in Pages

Step	Command	Description
Enter the global configuration mode.	<b>enable</b>	-
Configure Display of Properties in Pages	<b>more { on   off   displine [ num ] }</b>	Mandatory By default, the function of display in pages is enabled. By default, 24 lines are displayed in <b>displine</b> .

## 7.2.10 Operation record file management

### Configuration Condition

None

### Configure Operation Record File

Operation records are saved in flash by default, and operation record file management is mainly to change the location where operation records are saved.

Table 7-13 Configuring File Encryption and Operation Record Encryption

Step	Command	Description
Enter the global configuration mode.	<b>config terminal</b>	-
Operation record file management	<b>shell-history location</b> <i>device-name</i>	User-specified location for saving operation records.
Operation record file size specification.	<b>shell-history file max-size</b> <i>num</i>	Users specify the size of the operation record file.

## 7.2.11 Configure system security mode.

### Configuration Condition

None

### Configure system security mode.

Table 7-14 Configuring System Security Mode

Step	Command	Description
Enter the global configuration mode.	<b>config terminal</b>	
Configure system security mode.	<b>ssac mode</b> <i>{strict   loose}</i>	The system security mode can be configured as strict mode or loose mode.

## 7.2.12 System Managing, Monitoring, and Maintaining

Table 7-15 System Managing, Monitoring, and Maintaining

Command	Description
<b>show clock</b>	Display system clock information.
<b>show cpu</b>	Display CPU occupancy information.
<b>show device</b>	Display system device information.
<b>show environment</b>	Display board temperature information.
<b>show history</b>   { <b>begin</b> <i>expression</i>   <b>exclude</b> <i>expression</i>   <b>include</b> <i>expression</i>   <b>redirect</b> { <b>file</b> <i>file-name</i>   <b>ftp</b> [ <b>vrf</b> <i>vrf-name</i> ] { <i>hostname</i>   <i>ip-address</i> } <i>user-name password file-name</i>   <b>ftps</b> [ <b>vrf</b> <i>vrf-name</i> ] { <i>hostname</i>   <i>ip-address</i> } <i>user-name password file-name</i> } }	Display history command information.
<b>show language</b>	Display system language version information.
<b>show login-secure</b> { <b>telnet</b>   <b>ssh</b>   <b>ftp</b>   <b>snmp</b> }{ <b>ip-addr</b>   <b>user</b>   <b>quick-connect</b> }	Display system login security service Information.
<b>show login-secure quick-connect</b>	Display quick connection information for system login security.

Command	Description
<b>show mbuf allocated</b> [ <i>pool-name</i> ]	Display mbuf information.
<b>show memory</b>	Display memory information.
<b>show pool</b> [ <b>detail</b>   <b>information</b> ]	Display system memory pool information.
<b>show process</b> [ <i>task-name</i> ]	Display the main tasks in the system and their running status.
<b>show semaphore</b> { <i>sem-name</i>   <b>all</b>   <b>binary</b>   <b>counting</b>   <b>list</b>   <b>mutex</b> } [ <b>any</b>   <b>pending</b>   <b>unpending</b> ]	Display system semaphore information.
<b>show spy</b>	Display monitoring switch status.
<b>show stack</b>	Display the usage of each task stack in the system.
<b>show system fan</b> [ <b>brief</b> ]	Display system fan information.
<b>show system lpu</b> [ <i>lpu-num</i>   <b>brief</b> ]	Display system LPU information.
<b>show system module brief</b>	Display summary information for all module components of the device.
<b>show system mpu</b> [ <b>brief</b>   <i>mpu-num</i> ]	Display system MPU information.
<b>show system power</b> [ <i>power-num</i>   <b>brief</b> ]	Display system power information.
<b>show tech-support</b> { <b>sys-base</b> [ <b>detail</b> ]   <b>drv-base</b> [ <b>detail</b> ]   <b>I2-base</b> [ <b>detail</b> ]   <b>I3-base</b> [ <b>detail</b> ]   <b>all</b> } [ <b>page</b>   <b>to-memory</b>   <b>to-flash</b> ]	Display technical support information.
<b>show version</b> [ <b>detail</b> ]	Display system version information.

### 7.2.13 Configure the flexible table entry mode.

#### Configuration Condition

None

#### Configure the flexible table entry mode.

Flexible table entry mode is configured to adjust some of the device's table entry specifications, such as MAC address table, routing table, etc., for different scenarios.

Table 16-17 Configuring the Flexible Table Entry Mode

Step	Command	Description
Configure the flexible table entry mode.	<b>flexible-table mode</b> { <b>BALANCE</b>   <b>LARGE_L2</b>   <b>LARGE_ROUTE</b>   <b>MAC_ROUTE</b>   <b>ENHANCED</b> }	By default, the flexible table entry mode is BALANCE.

## 7.3 Typical Configuration Example of System Management

### 7.3.1 Configure user- and IP-based login restrictions

#### Network Requirements

- PC1 and PC2, as local terminals, can log in to Device via Telnet and ssh.
- Device can restrict login to PC1 and PC2 by user and IP.

#### Network Topology

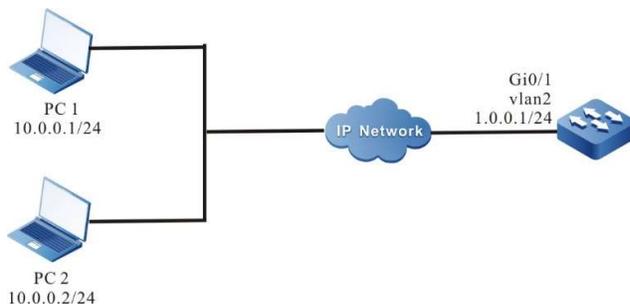


Figure 7-1 Network Topology for Configuring User- and IP-based Login Restrictions

#### Configuration Steps

- Step 1: Configure the IP address of each interface and configure the routing protocol to enable intercommunication between PC1, PC2 and Device. (Omitted)
- Step 2: Configure the user- and IP-based login restriction function.

#Enable telnet, ssh login security function.

```
Device#configure terminal
Device(config)#service login-secure telnet
```

```
Device(config)#service login-secure ssh
```

#Configure the maximum number of retries to 5 for telnet and ssh IP addresses and 5 for users, respectively.

```
Device(config)#login-secure telnet ip-addr max-try-time 5
Device(config)#login-secure telnet user max-try-time 5
Device(config)#login-secure ssh ip-addr max-try-time 5
Device(config)#login-secure ssh user max-try-time 5
```

Step 3: Enable the ssh service of Device, configure the username and password, and set up local login authentication.

```
Device(config)#ip ssh server
Device(config)#local-user user1 class manager
Device(config-user-manager-user1)#service-type ssh
Device(config-user-manager-user1)#password 0 admin
Device(config-user-manager-user1)#exit
Device(config)#line vty 0 15
Device(config-line)#login aaa
Device(config-line)#exit
```

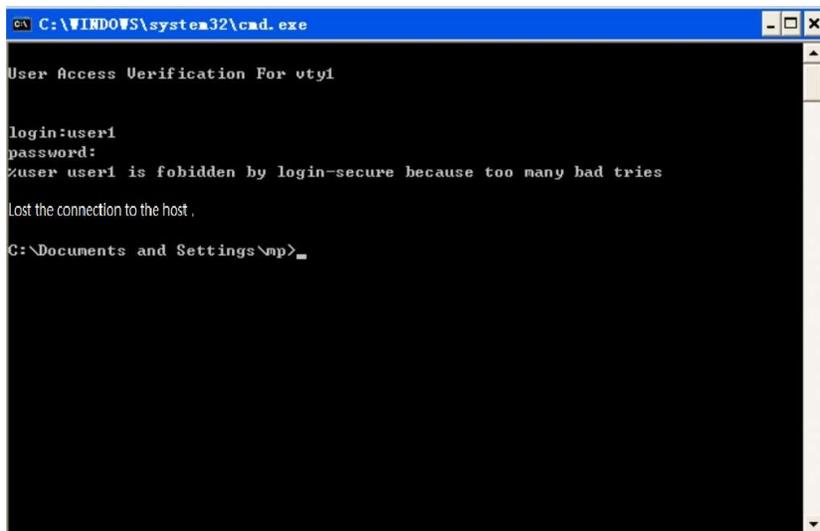
Step 4: Check the result.

#PC1 attempts to log in to Device via telnet with username user1, and after entering the wrong password 6 times in a row, the user information of the telnet login security statistics is displayed on Device:

```
Device#show login-secure telnet user
telnet module forbidden user information:
user      try-time  forbid-time  number  record-time
-----
user1     6         00:09:00     0       00:01:00
```

You can see that user1 is considered as a login attack user and is not allowed to login to the device via telnet for 10 minutes.

PC1 uses user1 to log in to Device via telnet for the second time, the system prompts that login is rejected.



#PC2 attempts to log in to Device via ssh, using unconfigured username of Device, and after logging in 6 times in a row, the ip information in the ssh login security statistics is displayed:

```
Device#show login-secure ssh ip-addr
```

```

ssh module forbidden login address:
client address try-time forbid-time type number record-time
-----
10.0.0.2 6 00:09:00 login 0 00:01:00

```

You can see that PC2's IP address is considered to be a login attack address, and PC2 is not allowed to log in to the device via ssh for 10 minutes.

At this point, PC2 logs in to Device via ssh again and will be prompted that login is rejected.

---

## Note

- When the number of logins exceeds the configured maximum number of retries, it will be considered a login attack and rejected of login; logins equal to the configured maximum will not be forbidden.
  - Some ssh clients on the PC will retry internally when login fails, and the device will still record this as multiple logins.
  - By default, the telnet and ssh login security functions of the device are enabled.
- 

### 7.3.2 Configure quick login restrictions

#### Network Requirements

- PC1 and PC2, as local terminals, can log in to Device via Telnet.
- PC1 is restricted from logging in after repeated quick logins to Device, while PC2 is not affected.

#### Network Topology

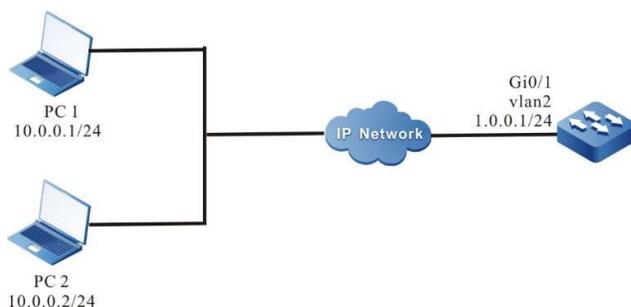


Figure 2-7 Network Topology for Configuring Quick Login Restriction

#### Configuration Steps

- Step 1: Configure the IP address of each interface and configure the routing protocol to enable intercommunication between PC1, PC2 and Device. (Omitted)
- Step 2: Configure telnet quick login restriction function.

#Enable telnet login security function and configure the maximum number of quick logins to 20 and forbid time to 10.

```
Device#configure terminal
Device(config)#service login-secure telnet
Device(config)#login-secure telnet quick-connect max-times 20
Device(config)#login-secure telnet quick-connect forbid-time 10
```

Step 3: Configure the login username and password of Device , and set it to use local authentication to log in.

```
Device(config)#local-user user1 class manager
Device(config-user-manager-user1)#service-type ssh
Device(config-user-manager-user1)#password 0 admin
Device(config-user-manager-user1)#privilegeprivilege 15
Device(config)#line vty 0 15
Device(config-line)#login aaa
Device(config-line)#exit
```

Step 4: Check the result.

#PC1 logs in and out via telnet for 21 times repeatedly using user1, with no more than 30 seconds between each login, the quick connection information in the telnet login security statistics is displayed:

```
Device#show login-secure telnet quick-connect
telnet module quick connect info:
connect ip      connect times  last connect time      forbid-time  record-time
-----
10.0.0.1       21           TUE AUG 11 20:22:38 2015 00:09:00    00:01:00
```

You can see that PC1 is considered as a login attack address and is not allowed to login to the device via telnet for 10 minutes.

PC2 can successfully log in to Device via telnet.

# 8 System Alarm

---

## 8.1 Overview

With the system alarm function, if an exception occurs, the system sends an alarm prompt message so that the user can pay attention to the exception of the device and take the corresponding measures to ensure stable operation of the device. System alarms include temperature alarms, power supply abnormality alarms, and fan abnormality alarms. For the system temperature alarms, if the CPU or environment temperature reaches the threshold, abnormal system alarm log information is generated. By default, the CPU temperature alarm threshold is 110°C and the environment temperature alarm threshold is 110°C. Power supply and fan exceptions also generate abnormal system alarm log information.

## 8.2 System Alarm Function Configuration

Table 8-1 System Alarm Function Configuration List

Configuration Task	
Configure System Temperature Alarms	Configure System Temperature Alarms
Configure System CPU Alarms	Configure System CPU Alarms
Configure System Memory Alarms	Configure System Memory Alarms
Configure System Power Supply Alarms	Configure System Power Supply Alarms
Configure System Fan Alarms	Configure System Fan Alarms

### 8.2.1 Configure System Temperature Alarms

#### Configuration Condition

Before configuring system alarms, ensure that:

- After the system is started and operates stably, all boards are loaded successfully.
- After the system is started and operates stably, the power supply and fans operate normally.

### Configure System Temperature Alarms

Configure the system temperature alarms is to configure the system switch chip, CPU and motherboard alarm temperature, when the switch chip, CPU or motherboard temperature reaches a certain threshold value, the system alarm log message will be generated.

Table 8-2 Configuring System Temperature Alarms

Step	Command	Description
Enter the global configuration mode.	<b>config terminal</b>	-
Configure switch chip, CPU or motherboard temperature alarm thresholds	<b>alarm temperature { mpu   lpu   sfu }{ switch   cpu   inletair} temperature</b>	Mandatory
Configure the temperature alarm threshold of an active virtual switch member device's switch chip, CPU or motherboard in a stacked environment.	<b>alarm temperature device device-num { mpu   lpu   sfu }{ switch   cpu   inletair} temperature</b>	Mandatory

### 8.2.2 Configure System CPU Alarms

#### Configuration Condition

Before configuring system alarms, ensure that:

- After the system is started and operates stably, all boards are loaded successfully.

#### Configure System CPU Alarms

Configure system CPU alarms is the function that sends an CPU utilization exception alarm when the monitoring threshold is exceeded after the threshold of CPU utilization monitoring is configured.

Table 8-3 Configuring System CPU Alarms

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the system CPU utilization alarm threshold	<b>cpu utilization warn- threshold [ rate-value ]</b>	Optional

### 8.2.3 Configure the low threshold of memory usage

#### Configuration Condition

Before configuring the system threshold alarms, first complete the following tasks:

- After the system is started and operates stably, all boards are loaded successfully.

#### Configure the Low Threshold of Memory Usage

Configure the low threshold of system memory usage refers to the function that sends the system into a state of memory shortage when the system memory falls below the low threshold after the low threshold of system memory usage is configured.

Table 4-8 Configuring System Memory Threshold Alarms

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure system memory threshold alarms.	<b>memory threshold low low-value</b>	Optional  By default, the low threshold of system memory is 64M.

### 8.2.4 Configure System Memory Alarms

#### Configuration Condition

Before configuring system alarms, ensure that:

- After the system is started and operates stably, all boards are loaded successfully.

#### Configure System Memory Alarms

Configuring system memory alarms is a function that alerts you of system memory utilization exception when the monitoring threshold is exceeded after the system memory utilization monitoring threshold is configured.

Table 8-5 Configuring System Memory Alarms

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the system memory utilization alarm threshold	<b>memory utilization warner-threshold</b> [ <i>rate-value</i> ]	Optional By default, the system memory utilization alarm threshold is 95%.

## 8.2.5 Configure System Power Supply Alarms

### Configuration Condition

None

### Configure System Power Supply Alarms

If a power supply fault or exception occurs, the system immediately generates log information about system power supply alarms. This helps the user to pay attention to the exception of the device power supply and take the corresponding measures to get rid of the fault and ensure stable operation of the device. By default, the system power supply alarm function is enabled.

## 8.2.6 Configure System Fan Alarms

### Configuration Condition

None

### Configure System Fan Alarms

If a system fan fault or exception occurs, the system immediately generates log information about the system fan alarm. This helps the user to pay attention to the exception of the device fans and take the corresponding measures to get rid of the fault and ensure stable operation of the device. By default, the system fan alarm function is enabled.

# 9 System Log Configuration

---

## 9.1 Overview

System log information is categorized into eight levels, including: **emergencies**, **alerts**, **critical**, **errors**, **warnings**, **notifications**, **informational**, and **debugging**. Here levels 0-6 are log information and level 2 is debugging information. For details, refer to the following table.

Table9-1 Description of the System Log Level Fields

Field	Level	Description
<b>emergencies</b>	0	Fatal fault. The system is unavailable, the device stops and it needs to be restarted.
<b>alerts</b>	1	Serious error. Functions of a certain type become unavailable, and the services are stopped.
<b>critical</b>	2	Critical error. Irreversible problems occur on the functions of a certain type, and some functions are affected.
<b>errors</b>	3	Error Message
<b>warnings</b>	4	Warning message.
<b>notifications</b>	5	Event notification message.
<b>informational</b>	6	Message prompt and notification.
<b>debugging</b>	7	Debugging message.

System log information is outputted to five directions: control console (Console terminal), monitor console (Telnet or SSH terminal), log server, log files (memory log files and flash log files) and email. The output to the five directions is controlled by respective configuration commands. The debugging information is outputted to two directions, control console and monitor console. In some special cases, the debugging information can also be configured to output to the log server or log files.

Table 9-2 Directions for Log Output

Log Output Direction	Description
Control console	System log information is outputted to the Console terminal.
Monitor console	System log information is outputted to the Telnet or SSH terminal.
Log server	System log information is outputted to the log server.  By default, logs of levels 0-5 are outputted to the log server.
Log files	System log information is outputted to the system memory or flash memory.  By default, log information of levels 0-5 is outputted to the system memory, and log information of levels 0-5 is outputted to the flash memory.
email	System log information is outputted to the log email.  By default, logs of level 0~4 are outputted to the log email.

The log module runs in a separate syslog process. The main thread of the syslog process receives the log information sent from the system, first processes the log data and allocates cache space, and then mounts it to the cache queue corresponding to each output terminal according to the configured output action. Since the cache queue has a length limit, there is a situation that logs are lost when a large number of logs are outputted. In such case, the log module will count the lost logs. There are two threads for log scheduling output (log information output to console, monitor, log server and log file run in the same sub-thread, and log information output to email runs in another sub-thread), and a timer is enabled in the scheduling thread for each output direction, and the timer gets log data from the queue corresponding to the terminal after each response and outputs it to the corresponding terminal as configured by the user.

## 9.2 System Log Function Configuration

Table 9-3 Log Function Configuration List

Configuration Task	
Configure Log Output Functions	Configure Log Output to the Control Console
	Configure Log Output to the Monitor Console
	Configure Log Output to the Server
	Configure Log Output to Files
	Configure log output to email
Configure the Timestamp for Logs	Configure the Timestamp for Logs
Configure operation log output to the log server	Configure operation log output to the log server
Configure log duplicate suppression function	Configure log suppression
Configure log files capacity	Configure log files capacity
Configure log files encryption function	Configure log files encryption
Configure log display color	Configure log display color
Configure log filtering function	Configure log filtering function
Configure the origin-id of a device	Configure the origin-id of a device

### 9.2.1 Configure Log Output Functions

#### Configuration Condition

None

#### Configure Log Output to the Control Console

The control console refers to a Console terminal. It is a channel through which the system output log information to the control console.

Table 9-4 Configuring Log Output to the Control Console

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable the log output function.	<b>logging enable</b>	Optional By default, the log output function is enabled.
Enable log display on the control console.	<b>logging source</b> { <i>module-name</i>   <b>default</b> } <b>console</b> { <b>level</b> <i>severity</i>   <b>deny</b> }	Optional By default, log display on the control console is enabled.

### Configure Log Output to the Monitor Console

The monitor console refers to the Telnet or SSH terminal, which is used for managing remote devices. When configuring to display log output to the monitor console, the log display on the current terminal shall be enabled.

Table 9-4 Configuring Log Output to the Monitor Console

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable the log output function.	<b>logging enable</b>	Optional By default, the log output function is enabled.
Enable log display on the monitor console.	<b>logging source</b> { <i>module-name</i>   <b>default</b> } <b>monitor</b> { <b>level</b> <i>severity</i>   <b>deny</b> }	Optional By default, log display function of the global control console is enabled.
Enable log display on the current monitor console.	<b>terminal monitor</b>	Mandatory By default, log display function of the current control console is not enabled.

### Configure Log Output to the Server

In order to record log information more comprehensively, you can configure log output to the log server for easy maintenance and management of the system. When configuring log output to the log server, the host address or domain name of the log server shall be configured.

Table 9-5 Configuring Log Output to the Log Server

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable the log output function.	<b>logging enable</b>	Optional By default, the log output function is enabled.
Configure Log Output to the Log Server	<b>logging server</b> <i>server-name</i> [ <b>vrf</b> <i>vrf-name</i> ] { <b>ip</b> <i>ip-address</i>   <b>ipv6</b> <i>ipv6-address</i> / <b>hostname</b> <i>host-name</i> } [ <b>port</b> <i>port-num</i> ] [ <b>facility</b> <i>facility-name</i> ] [ <b>level</b> <i>severity</i> ]	Mandatory By default, log output to the log server is not enabled.
Configure Log Output to Source IP Address.	<b>logging server source</b> { <b>ip</b> <i>ip-address</i>   <b>ipv6</b> <i>ipv6-address</i>   <b>interface</b> <i>interface-name</i> }	Optional By default, the outgoing interface for sending log information will be determined based on the route, and the primary IP address of the outgoing interface will be used as the source IP address for the log output.
Configure a Specified Level of Log Output to the Log Server	<b>logging source</b> { <i>module-name</i>   <b>default</b> } <b>server</b> [ <i>server-name</i> &<1-8> ] { <b>level</b> <i>severity</i>   <b>deny</b> }	Optional By default, logs of level 0-5 are outputted to the log host.

### Configure Log Output to Files

Log files can be stored either in memory or in Flash storage. For log information stored in memory, only the content from after the syslog is started until before the system or the syslog process is restarted is kept. By

default, log information at level 5 (**notifications**) and above is kept. The log information stored in Flash memory is saved as level 5 (**notifications**) and above by default, please refer to the detailed definition in Table 9-1 for log levels. When the log file size reaches the configured maximum capacity, the oldest log file will be deleted first when adding a new log (log information is recorded by multiple log files), and then a new log file will be created and the new log information will be recorded into the new log file.

Table 9-6 Configuring Log Output to Files

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable the log output function.	<b>logging enable</b>	Optional By default, the log output function is enabled.
Configure Log Saved to Flash	<b>logging source { module-name   default } file { level severity   deny }</b>	Optional By default, logs of level 0-5 are saved to Flash.
Configure Log Saved to Memory	<b>logging source { module-name   default } buffer { level severity   deny }</b>	Optional By default, logs of level 0-5 are saved to memory.
Configure Log Files Capacity Alarms	<b>logging { buffer / file } warning warning-value recover-value</b>	Optional By default, the log information alarm threshold is at 90% and the recovery threshold is at 70%.
Configure Log Files Compression	<b>logging compress [ gunzip ]</b> <b>logging compress maximum value</b>	Optional By default, log compression function is not enabled.

### Configure Log Output to Email

In order to record log information more comprehensively, you can configure log information to be outputted to the corresponding recipient and copy-to email address via email.

Table 9-7 Configuring Log Output to Email

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable the log output function.	<b>logging enable</b>	Optional By default, the log output function is enabled.
Configure Email Template	<b>logging email</b> <i>email-profile</i>	Mandatory By default, the template for log output to the email is not configured.
Configure the email address of the recipient receiving the log information.	<b>mail recipient</b> <i>mail-address</i>	Mandatory By default, the email address of the recipient receiving the log information is not configured.
Configure the copy-to email address receiving the log information.	<b>mail copyto</b> <i>mail-address</i>	Optional By default, no copy-to email address receiving the log information is configured.
Configure the email address of the sender of the log information.	<b>mail sender</b> <i>mail-address</i>	Mandatory By default, not email address of the sender of the log information is configured.
Configure the email password of the sender of the log information.	<b>mail sender password</b> <i>password-string</i>	Mandatory By default, no email password of the sender of the log information is configured.

Step	Command	Description
Configure the email domain address of the recipient receiving the log information.	<b>mail server</b> <i>server-name</i>	Optional By default, the characters after the @ character in the sender's email address are used as the sender's domain address.
Configure the email subject of the sender of the log information.	<b>mail subject</b> <i>subject-name</i>	Optional By default, no email subject of the sender of the log information is configured.
Configure a specified level of log information to be outputted to the corresponding recipient and copy-to email address via email.	<b>logging source</b> { <i>module-name</i>   <b>default</b> } <b>email</b> { <b>level</b> <i>severity</i>   <b>deny</b> }	Optional By default, logs of level 0-4 are outputted to email.

## 9.2.2 Configure the Timestamp for Logs

### Configuration Condition

None

### Configure the Timestamp for Logs

Timestamp for logs provides a detailed record of when the log was generated. By default, the log timestamp takes the form of absolute time, but it also supports the form of Uptime (relative time). When configuring absolute time, you can specify the year of logging and log with millisecond precision, with detailed log time output.

Table 9-8 Configuring Timestamp for Logs

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the Type of Timestamp for Logs	<b>logging timestamps uptime</b>	Optional By default, the log information uses the absolute timestamp.
Configure the Type of Timestamp for Logs	<b>logging timestamp-format { msec   timezone   year }</b>	Optional By default, log information is displayed in a timestamped format with the year of logging.

### 9.2.3 Configure Operation Log Output to the Log Host

#### Configuration Condition

Configure log output to the log host first.

#### Configure operation log output to the log server

When the operation log is configured to be sent to the log server, you can view the user-generated operation log on the log server.

Table 9-9 Configuring Log Output to the Log Host

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable the log output function.	<b>logging enable</b>	Optional By default, the log output function is enabled.
Configure Log Host	<b>logging server <i>server-name</i> [ vrf <i>vrf-name</i> ] { ip <i>ip-address</i>   ipv6 <i>ipv6-address</i>   hostname <i>host-name</i> }</b>	Mandatory By default, the function of sending logs to the

Step	Command	Description
	[ <b>port</b> <i>port-num</i> ] [ <b>facility</b> <i>facility-name</i> ] [ <b>level</b> <i>severity</i> ]	log server is not enabled.
Configure operation log output to the log server	<b>logging operation to-server</b>	Mandatory By default, the function of sending operation logs to the log server is not enabled.

## 9.2.4 Configure log suppression

### Configuration Condition

None

### Configure Log Duplicate Suppression

Since in some cases the module may keep outputting the same logs over and over again, affecting the observation of other logs, this can be avoided by enabling the log duplicate suppression function. Repeated log information are outputted once within each suppression cycle, and the number of times this log was suppressed during the suppression cycle is outputted at the end of the suppression cycle.

Table 9-11 Configuring Log Duplicate Suppression

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the function of log duplicate suppression.	<b>logging suppress duplicates interval</b> <i>interval-num</i>	Mandatory By default, the function of log suppression is enabled.

## 9.2.5 Configure log files capacity

### Configuration Condition

None

### Configure log files capacity

Due to the limitation of Flash memory capacity, the log file capacity can be configured in the range of 1M to 32M. When the log information storage exceeds the configured maximum capacity limit, new logs will overwrite the old log information (overwrite the old log information file in file units).

Table 9-10 Configuring Log Files Capacity

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure log files capacity	<b>logging file size</b> <i>file-max-size</i>	Optional By default, the log files capacity is 1M bytes.

## 9.2.6 Configure log files encryption

### Configuration Condition

None

### Configure log files capacity

Considering the security of log information, the log files stored in flash can be encrypted. When the log files encryption function is configured, the logs generated subsequently will be stored in the form of cipher text in the log files. If the password of the log files is changed, logs previously stored in the form of cipher text will not be displayed in plain text. The log information will be displayed in plain text only when the password is reconfigured to the password used to generate the logs.

Table 9-11 Configuring Log Files Encryption

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure log files encryption	<b>logging file encryption</b> <i>algorithms SMV4 key</i> <i>password</i>	Optional By default, no encryption is configured for the log files in Flash.

## 9.2.7 Configure log display color

### Configuration Condition

None

### Configure log display color

When displaying log information, different levels of log information can be configured to display different colors in order to highlight the importance of the information. By default, the function of log display color is enabled and different log levels correspond to default log display colors, please refer to the following table:

Table 9-12 Log Colors Description

Field	Description
<b>emergencies</b>	Red
<b>alerts</b>	Purple
<b>alerts</b>	Blue
<b>errors</b>	Brown
<b>warnings</b>	Cyan
<b>notifications</b>	White
<b>informational</b>	Green
<b>debugging</b>	Green

Table 9-13 Configuring Log Display Color

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure log display colors corresponding to log levels	<b>logging color</b> [ <i>logging-level</i> <i>logging-color</i> ]	Optional By default, each log level has its default log display color.

### Note

- When the control or monitoring console needs to output the color of log information, the color option of the display terminal shall be configured, otherwise, the color of the log information cannot be displayed.

## 9.2.8 Configure log filtering function

### Configuration Condition

None

### Configure log filtering function

When configuring log filtering, you can specify to display not only log information containing the filter string, but also log information without the filter string and the log information level range. When this command is used, the filter string needs to be used together with the log level range.

Table 9-14 Configuring the Log Filtering Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure log filtering function	<b>logging filter</b> { <b>exclude</b> <i>exclude-string</i>   <b>include</b> <i>include-string</i>   <b>level</b> <i>high-level low-level</i> }	Optional By default, the log filtering function is not enabled.

## 9.2.9 Configure the origin-id of a device

### Configuration Condition

None

### Configure the origin-id of a device

When configuring the origin-id of a device, a maximum 63 characters can be configured. After configuring, the hostname field of the logs sent to the log server will be replaced by the origin-id string.

Table 9-15 Configuring the Origin-id of a Device

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the origin-id of a device	<b>logging origin-id string</b> <i>origin-id</i>	Optional By default, the origin-id of a device is not configured.

## 9.2.10 Log Monitoring and Maintaining

Table 9-16 Log Monitoring and Maintaining

Command	Description
<b>clear logging</b> [ <b>buffer</b>   <b>file</b> ]	Clear log information stored in memory or Flash.
<b>show logging</b> [ <b>buffer</b>   <b>file</b> ]	Display log information stored in memory or Flash.
<b>show logging</b> { <b>file</b>   <b>buffer</b> } <b>desc</b>	Reverse display of log information stored in memory or Flash.
<b>show logging filter</b>	Display log filtering configuration information.
<b>show logging operation</b>	Display log information stored in the operation log files.
<b>show logging</b> [ { <b>file</b>   <b>buffer</b> } [ <b>begin-level</b> <i>level-value</i> / [ <b>start-time</b> <i>stime</i> [ <b>end-time</b> <i>etime</i> ] ] [ <b>detail</b> ] ] ]	Display log information stored in the operation log files, and with the filtering option of time and level to display filtered log information.
<b>show logging</b> { <b>file</b>   <b>buffer</b> } <b>message-counter</b>	Display the size of the log files and the number of log entries stored in Flash or memory of the device.

# 10 Software Upgrade

---

## 10.1 Overview

Software upgrade provides a more stable software version and more abundant software features for the user.

Upgraded programs are stored in the storage mediums of the device in the form of files or data blocks. The software modules with different functions cooperate to keep the device in the stable working state and support the hardware features of the device and application services of users.

Users can upgrade software through the TFTP/FTP network transmission mode or the YmodemYmodem transmission mode of the Console port. In upgrading software of different types, users must carefully read the operation steps and notes and cautions described in the manuals related to the software upgrade.

In upgrading software, you usually need to upgrade software of each type. If the software of a type is not updated during the upgrade process, you need not upgrade the software again. Usually, you can restart the device only after the all software versions are upgraded.

The following types of software are available:

- **Image package:** A MPU package with the .pck suffix contains a collection of programs (operating system, applications, etc.) for the normal operation of the system.
- **CMM program:** Chassis Management Module (CMM) program with the suffix .bin or .pck. The CMM is responsible for monitoring the frame power and fan status, and providing status information of related boards.
- **FPGA (Field Programmable Gate Array) program:** The program with the suffix .bin is mainly used to implement the logic control of the device and the sending and receiving of service data.
- **Bootloader program:** A program with the suffix .bin or .pck. MPU bootloader program is cured in the ROM of the MPU and SPU, and is the first to be executed after the device is powered on. This program initializes the base system and its main function, and is mainly used to guide the operating system to load.
- **CPLD (Complex Programmable Logic Device) programs,** with the suffix .pck, are digital integrated circuits that construct logic functions.

- **Devinfo:** OEM program containing information such as model ID and function ID of various devices and boards. It is mainly used for upgrading when the equipment is retrofitted.
- **Patch:** Patch is a fast, low-cost way to fix defects in product software versions. The main advantage of patching over upgrading software versions is that it does not disrupt the business that the device is currently running, i.e., defects in the current software version of the device can be fixed without rebooting the device.
- **Package packager:** A package file containing image, bootloader, cmm programs, which allows for upgrade of multiple types of software programs at once, convenient and time-saving.

The correspondence between the above-mentioned types of upgrade software and types of board is shown in the table:

Table 10-1 Correspondence between Upgrade Software and Different Types of Boards

	image Package	cmm Procedures	fpga Procedures	bootload Procedures	cpld Procedures	devinfo DOCUMENTATION	patch DOCUMENTATION	package Package file
Main Process ing Unit ( MPU)	√	√	√	√	√	√	√	√
S P U m o t h er	-	√		√	√-			√

	image Packag e	cmm Proc edur es	fpga Proc edur es	bootload Procedur es	cpld Proc edur es	devinfo DOCUM ENTATI ON	patch DOCU MENT ATION	package Package file
ca rd								
S P U d a u g ht er ca rd	-	√		√	√-			√
F or w ar di n g b o ar d	-	√		√	√-			√

---

 **Note**

- WAN business board daughter cards like CPOS, POS, etc. have FPGA program, while Ethernet business board daughter cards does not have FPGA program.
- 

## 10.2 Software Upgrade Function Configuration

Table 10-2 Software Upgrade Function Configuration List

Configuration Task	
Upgrade the image Program Package	Upgrade MPU iamge package via TFTP/FTP
CMM program upgrade	Upgrade CMM program via TFTP/FTP
FPGA program upgrade	Upgrade FPGA program via TFTP/FTP
bootloader Program Upgrade	Upgrade bootloader program via TFTP/FTP
CPLD program upgrade	Upgrade CPLD program via TFTP/FTP
Devinfo file upgrade	Upgrade devinfo file package via TFTP/FTP
Patch file upgrade	Patch upgrade via TFTP/FTP
Package packager upgrade	Upgrade package packager via TFTP/FTP

### 10.2.1 Upgrade the image Program Package

The image package is suitable for MPU upgrade.

#### Configuration Preparation

Before upgrading the image program package, ensure that:

- Ensure that the route between the TFTP/FTP server and the device interface is reachable and the route can be pinged through.
- The TFTP/FTP server configuration is correct, and the image program is stored in the specified directory of the TFTP/FTP server.
- Ensure the remaining flash space is sufficient. If the space is insufficient, manually delete files on flash that are not in use.
- The configuration files have been backed up.

#### Upgrade the image Program Package in TFTP/FTP Mode

Enter the privileged user mode, ensure that the device can obtain the upgrade program through the external TFTP/FTP server, and then use the sysupdate image command to upgrade the program package.

Table 10-3 Upgrading the image Program Package in TFTP/FTP Mode

Step	Command	Description
Enter the privileged user mode.	None	Mandatory

Step	Command	Description
Upgrade the image program package.	<b>sysupdate image [ device { memberId   all } ] mpu { cardNo   all } [ vrf vrf-name ] { dest-ip-address   dest-ipv6-address } filename [ ftp ftp-username ftp-password ] [ reload ]</b>	Mandatory  If the FTP option is not specified, TFTP is used for upgrade by default.

For example: In standalone mode, upgrade the active/standby MPU image program via the FTP server 130.255.168.45.

```

Hostname#sysupdate image mpu all 130.255.168.45 sp9a-g-9.7.1.1(74)(R).pck ftp a a
#The device will prompt the following:

checking "sp9a-g-9.7.1.1(74)(R).pck" : ...OK
The file sp9a-g-9.7.1.1(74)(R).pck already exists on Mpu 0, overwrite it?(Yes|No):y
downloading "sp9a-g-9.7.1.1(74)(R).pck" :
#####
#####OK
Download "sp9a-g-9.7.1.1(74)(R).pck" (144531060 Bytes) successfully.
Verify the image...
Apr 16 2021 12:35:05 switch MPU0 %SYS_UPDATE-RESULT-5:image : Mpu 0 download file successfully!valid
Writing file to
filesystem.....
.....OK!
Start backup ios to raw flash...
Apr 16 2021 12:36:05 switch MPU0 %SYS_UPDATE-RESULT-5:image : Mpu 0 write file to file-system successfully!OK
%Sysupdate image is in process, please wait...
Apr 16 2021 12:36:37 switch MPU0 %SYS_UPDATE-RESULT-5:image : Mpu 0 write file to backup file-system successfully!
Apr 16 2021 12:36:37 switch MPU0 %SYS_UPDATE-RESULT-5:image : Mpu 0 upgrade successfully!
%Sysupdate image finished.

sysupdate image result information list:
-----
Card    result information
-----
Mpu 0   upgrade successfully!
Mpu 1   upgrade successfully!

```

May 21 2020 08:48:26 SWICTH MPU0 %SYS\_UPDATE-RESULT-5:Upgrade image to sp9a-g-9.7.1.1(74)(R).pck from ftp: 130.255.168.45 successfully !

#The above information indicates that the image program of the active/standby MPU has been successfully upgraded.

---

 **Note**

- If the command option reload is added, the system prompts whether to save the configuration and whether to restart the device. However, usually the device is started after all programs are
-

---

upgraded. Therefore, the reload option is not recommended.

- Before the upgrade, ensure that there is sufficient space in the flash. If the space is insufficient, the upgrade fails. In this case, you can manually delete files that are not in need from the flash memory to obtain more space for upgrading application programs.
  - When the active/standby MPU flash space is insufficient, it will prompt whether to delete the extra image file, if the space remains insufficient after deleting, the upgrade fails.
  - It takes a long time to upgrade the image program package. A smaller remaining space in the flash memory results in longer upgrade time.
  - After the upgrade is completed, to run the new image program, restart the device.
  - If there are two MPUs in the device, you need to upgrade them synchronously. If the versions of the two MPUs are inconsistent, it may lead to abnormal startup and operation.
  - When upgrading the active/standby MPU at the same time, the upgrade fails if one of them does not meet the upgrade conditions.
  - When upgrading the active/standby MPU simultaneously, the upgrade will continue when the standby MPU is not in position.
  - If the device fails to start normally, open the monitor screen, modify the startup mode to network startup. After the device is started successfully, start the upgrade. For the method, refer to the related section in the monitor configuration manual and command manual.
- 

---

## Warning

- During the upgrade process, ensure the device cannot be powered off, and avoid unplugging of the MPU or rebooting operation; otherwise, the system may not boot up and the flash file system of the MPU may be damaged.
- 

### 10.2.2 Patch program upgrade.

#### Configuration Condition

Before upgrading the patch program, the following tasks shall be completed:

- The route between the TFTP/FTP server and the device interface is reachable, and the TFTP/FTP server and the device can ping each other successfully.
- The TFTP/FTP server configuration is correct, and the patch program is stored in the specified directory of the TFTP/FTP server.
- The configuration files have been backed up.

#### Patch upgrade via TFTP/FTP

Enter the privileged user mode, ensure that the device can obtain the upgrade program through the external TFTP/FTP server, and then use the `sysupdate patch` command to upgrade the program package.

Table 10-4 Upgrading the Patch Program Package in TFTP/FTP Mode

Step	Command	Description
Enter the privileged user mode.	None	Mandatory
Upgrade patch program.	<b>sysupdate patch [device {memberId   all}] mpu {cardId   all } [ vrf vrf-name ] dest-ip-address filename [ ftp ftp-username ftp-password ]</b>	Mandatory  If the FTP option is not specified, TFTP is used for upgrade by default.

Upgrade the patch program with the file name sp9a-g-9.7.1.1.HP001.pat from the device interface via FTP server 130.255.168.45.

```
Hostname#sysupdate patch mpu all 130.255.168.45 sp9a-g-9.7.1.1.HP001.pat ftp a a
```

#The device will prompt the following:

```
checking "sp9a-g-9.7.1.1.HP001.pat" : ...OK
downloading "sp9a-g-9.7.1.1.HP001.pat" : #OK
Download "sp9a-g-9.7.1.1.HP001.pat" (16300 Bytes) successfully.
Update patch of master MPU:
Writing file to filesystem.....OK!

Patch update: operating, please wait for a moment
.....(Omitted).....

sysupdate patch to sp9a-g-9.7.1.1.HP001.pat from tftp: 130.255.168.4545 successfully !
```

#The above information indicates that the patch program of the device has been successfully upgraded, and the report and log information of the upgrade result will be outputted after the upgrade is completed.

### 10.2.3 CMM program upgrade

The CMM program is applicable to upgrading the MPU, forwarding board, SPU mother card and SPU daughter card.

#### Configuration Preparation

Before upgrading the CMM program, the following tasks shall be completed:

- Ensure that the route between the TFTP/FTP server and the device interface is reachable and the route can be pinged through.
- The TFTP/FTP server is correctly configured and the CMM program is correctly stored in the specified TFTP/FTP directory.
- The configuration files have been backed up.

#### Upgrade CMM program via TFTP/FTP

Enter privileged user mode, ensure that the device can get the upgrade program from external TFTP/FTP server, and then upgrade the program via sysupdate cmm command.

Table 10-5 Upgrading the CMM Program in TFTP/FTP Mode

Step	Command	Description
Enter the privileged user mode.	None	Mandatory
CMM program upgrade	<b>sysupdate cmm [ device { memberId   all } ] { { mpu   lpu   sfu } { cardNo   all }   all } [ vrf vrf-name ] { dest-ip-address   dest-ipv6-address } filename [ ftp ftp-username ftp-password ] [ reload ]</b>	Mandatory If the FTP option is not specified, TFTP is used for upgrade by default.

For example: In standalone mode, upgrade the CMM program of all active boards via the FTP server 130.255.168.45.

```

Hostname#sysupdate cmm all 130.255.168.45 sz02-cmm-tim4-1.0.1.4.pck ftp a a
#The device will prompt the following:
checking "sz02-cmm-tim4-1.0.1.4.pck" : ...OK
downloading "sz02-cmm-tim4-1.0.1.4.pck" : #OK
Download "sz02-cmm-tim4-1.0.1.4.pck" (361268 Bytes) successfully.
Update CMM of master MPU:Successfully!
Update CMM of LPU3:Successfully!
Update CMM of LPU7:Successfully!
Update CMM of LPU9:Successfully!
Update CMM of SFU1:Successfully!
%Sysupdate cmm is in process, please wait...
Apr 16 2021 13:43:09 switch MPU0 %SYS_UPDATE-RESULT-5:cmm : Mpu 0 download file successfully!
Apr 16 2021 13:43:09 switch MPU0 %SYS_UPDATE-RESULT-5:cmm : Mpu 0 upgrade successfully!
%Sysupdate cmm finished.

```

sysupdate cmm result information list:

```

-----
Card    result information
-----
Mpu 0   upgrade successfully!
Lpu 3   upgrade successfully!
Lpu 7   upgrade successfully!
Lpu 9   upgrade successfully!
Sfu 1   upgrade successfully!

```

#The above information indicates that the CMM program of the MPU, forwarding board, SPU mother card and SPU daughter card has been successfully upgraded.

### Note

- For business board daughter card, it is only shown when the upgrade fails.

- 
- The device needs to be rebooted after the CMM upgrade is completed.
- 

## Warning

- During the upgrade process, ensure that the device cannot be powered off, and avoid the unplugging of boards or rebooting operation; otherwise, the system may not be booted up.
  - You need to ensure that all boards share the same CMM version, otherwise it will lead to the system operation abnormality.
- 

### 10.2.4 bootloader Program Upgrade

The bootloader program is suitable for upgrading the MPU, forwarding board, SPU mother card and SPU daughter card.

#### Configuration Preparation

Before upgrading the bootloader program, you need to complete the following tasks:

- Ensure that the route between the TFTP/FTP server and the device interface is reachable and the route can be pinged through.
- The TFTP/FTP server is correctly configured and the bootloader program is correctly stored in the specified TFTP/FTP directory.
- The configuration files have been backed up.

#### Upgrade bootloader program via TFTP/FTP

Enter privileged user mode, ensure the device can get the upgrade program from external TFTP/FTP server, and then upgrade the program via `sysupdate bootloader` command.

Table 10-6 Upgrading the bootloader Program in TFTP/FTP Mode

Step	Command	Description
Enter the privileged user mode.	None	Mandatory
Upgrade bootloader program.	<b>sysupdate bootloader</b> [ <b>device</b> { <i>memberId</i>   <b>all</b> } ] {{{ <b>mpu</b>   <b>lpu</b>   <b>sfu</b> } { <i>cardNo</i>   <b>all</b> } }   <b>all</b> } [ <b>vrf</b> <i>vrf-name</i> ] { <i>dest-ip-</i> <i>address</i>   <i>dest-ipv6-</i> <i>address</i> } <i>filename</i> [ <b>ftp</b> <i>ftp-</i>	Mandatory  If the FTP option is not specified, TFTP is used for upgrade by default.

Step	Command	Description
	<code>username ftp-password ]</code> <code>[ reload ]</code>	

For example: In standalone mode, upgrade the bootloader program on all active MPUs simultaneously via the FTP server 130.255.168.45.

```

Hostname#sysupdate bootloader mpu all 130.255.168.45 sz02-bootloader-nl02-9.6.0.3ft15-1.1.18.pck ftp a
#The device will prompt the following:
checking " sz02-bootloader-nl02-9.6.0.3ft15-1.1.18.pck " : ...OK
downloading " sz02-bootloader-nl02-9.6.0.3ft15-1.1.18.pck " : ####OK
Download " sz02-bootloader-nl02-9.6.0.3ft15-1.1.18.pck " (3637108 Bytes) successfully.
Update bootloader start.
.....OK.

%Sysupdate bootloader is in process, please wait...
%Sysupdate bootloader finished.

sysupdate bootloader result information list:
-----
Card    result information
-----
Mpu 0   upgrade successfully!
Mpu 1   upgrade successfully!

```

#The above information indicates that the bootloader program of the active MPU has been successfully upgraded.

---

 **Note**

- When upgrading, please select the correct bootloader version, and upgrade the bootloader of all service boards on the device synchronously to avoid occurrence of exceptions.
- If the command option reload is added, the system prompts whether to save the configuration and whether to restart the device. However, usually the device is started after all programs are upgraded. Therefore, the reload option is not recommended.
- After the upgrade is complete, in order to run the new bootloader program, you need to reboot the board or the device.
- The bootloader program of all device MPUs need to be upgraded simultaneously to avoid the occurrence of exceptions.
- Please select the correct bootloader version for the upgrade to avoid the occurrence of exceptions.

---

 **Warning**

- During the upgrade process, ensure that the device cannot be powered off, and avoid unplugging of the MPU or rebooting operation; otherwise, the system may not boot up and the bootloader file of
-

---

the MPU may be damaged.

---

### Upgrade bootloader Program via Console

Ensure that the HyperTerminal can access the device through the Console port, enter the bootloader mode, adjust the baud rate, and upgrade through the ymodem of the HyperTerminal. If there are two MPUs on the device, they need to be upgraded separately.

For detailed descriptions of the commands, please refer to the relevant sections of the "bootloader" command manual.

Table 10-7 Upgrading the bootloader Program via the Console Port

Step	Command	Description
Set up the HyperTerminal.	None	Mandatory  Run the HyperTerminal program and select the corresponding serial port (e.g. com1), set up its properties, that is, baud rate is 9600 bps, soft flow control, 8 data bits, no parity check, 1 stop bit.
Enter the bootloader mode	None	Mandatory  When the device reboots, press CTRL+C to enter the bootloader mode.
Modify the baud rate of the Console port and the HyperTerminal to speed up the upgrade	<b>srate</b> { <i>speed</i> }	Optional  Modify the baud rate of the device Console port to 115200bps, then disconnect the HyperTerminal, modify the baud rate of the HyperTerminal to 115200bps, and reconnect.
Upgrade bootloader program.	<b>mupdate bootloader</b>	Mandatory  Enter the mupdate bootloader command in bootloader mode, then select the ymodem protocol in HyperTerminal,

Step	Command	Description
		select the bootloader program and start sending.

For example: Upgrade the bootloader program of the active MPU through the Console port.

```
#The device will prompt the following:
Download bootloader start...
Transferring sz03-bootloader-M-cn6x-1.0.77.pck,...
100% 1911 KB 3 KB/sec 00:08:17 0 Errors

## Total Size = 0x001ddd94 = 1957268 Bytes
Download bootloader OK.
bootloader image check:
..... done
Un-Protected 8 sectors

..... done
Erased 8 sectors
run command=cp,b 200000f8 0x17c00000 0xeb020
Copy to Flash... done
..... done
Protected 8 sectors
Update bootloader OK.

#The above information indicates that the bootloader program of the active MPU has been
successfully upgraded.
```

 **Note**

- Upgrade the bootloader program of the standby MPU through the Console port, the operation process is the same as the active MPU.
- When upgrading the bootloader program, make sure the speed rate of the HyperTerminal and the speed rate of the device Console port are in consistency.
- When upgrading the bootloader program, it is recommended to set the transfer rate to 115200bps, so as to shorten the upgrade transfer time.
- When upgrading the bootloader program, if the default rate of the Console port is modified, when loading the image package, the Console port rate of the device is automatically restored to 9600bps, and the rate of the HyperTerminal needs to be modified as well.
- It is recommended to try upgrading the bootloader program via TFTP/FTP, and use the Console port to upgrade the bootloader program only when the conditions for the former are not met.

 **Warning**

- During the upgrade process, ensure that the device cannot be powered off, and avoid the unplugging of the MPU or rebooting operation; otherwise, the system may not boot up and the bootloader file of the MPU may be damaged.

## 10.2.5 Devinfo file upgrade

The devinfo file is used for MPU upgrade.

### Configuration Preparation

The following tasks need to be completed before the devinfo file can be upgraded:

- Ensure that the route between the TFTP/FTP server and the device interface is reachable and the route can be pinged through.
- The TFTP/FTP server is correctly configured and the devinfo file is correctly stored in the specified TFTP/FTP directory.
- The configuration files have been backed up.

### Upgrade Devinfo Files via TFTP/FTP

Enter the privileged user mode to ensure the device can get the upgrade program from external TFTP/FTP server, and can be upgraded through sysupdate devinfo command.

Table 10-8 Upgrading devinfo File via TFTP/FTP

Step	Command	Description
Enter the privileged user mode.	None	Mandatory
Devinfo file upgrade	<b>sysupdate devinfo [ device { memberId   all } ] mpu { cardNo   all } [ vrf vrf-name ] { dest-ip-address   dest-ipv6-address } filename [ ftp ftp-username ftp-password ] [ reload ]</b>	Mandatory If the FTP option is not specified, TFTP is used for upgrade by default.

For example: In standalone mode, upgrade the devinfo files on all active/standby MPUs via the FTP server 130.255.168.45.

```

Hostname#sysupdate devinfo mpu all 130.255.168.45 devInfo(v2.2) ftp a a
#The device will prompt the following:
checking "devInfo(v2.2)": ...OK
downloading "devInfo(v2.2)": #OK
Download "devInfo(v2.2)" (6275 Bytes) successfully.
Writing file to filesystem....OK!

```

```

%Sysupdate devinfo is in process, please wait...
%Sysupdate devinfo finished.

```

```

sysupdate devinfo result information list:

```

```

-----
Card    result information
-----
Mpu 0   upgrade successfully!
Mpu 1   upgrade successfully!

```

---

#The above information indicates that the devinfo file of the active/standby MPU in position has been successfully upgraded.

---

### Note

- If the command option reload is added, the system prompts whether to save the configuration and whether to restart the device. However, usually the device is started after all programs are upgraded. Therefore, the reload option is not recommended.
  - After the upgrade is complete, in order to run the devinfo file, you need to reboot the board or the device.
  - The devinfo files of all active/standby MPUs on the device need to be upgraded in synchronization to avoid anomalies.
  - Please select the correct devinfo file version for the upgrade to avoid the occurrence of exceptions.
- 

---

### Warning

- During the upgrade process, ensure that the device cannot be powered off, and avoid the unplugging of MPU or rebooting operation; otherwise, the system may not boot up properly and the devinfo file may be damaged.
- 

## 10.2.6 Package file upgrade

The package file contains image, bootloader, cmm, and devinfo files, which can be upgraded all at once through the package file.

### Configuration Preparation

The following tasks need to be completed before the package file can be upgraded:

- Ensure that the route between the TFTP/FTP server and the device interface is reachable and the route can be pinged through.
- The TFTP/FTP server is correctly configured and the package file is correctly stored in the specified TFTP/FTP directory.
- The configuration files have been backed up.

### Upgrade Package Files via TFTP/FTP

Enter privileged user mode, ensure the device can get the upgrade program from external TFTP/FTP server, and then upgrade the program via sysupdate package command.

Table 10-9 Upgrading Package File via TFTP/FTP

Step	Command	Description
Enter the privileged user mode.	None	Mandatory
Upgrade Package File	<b>sysupdate package [ device { memberId   all } ] [ vrf vrf-name ] { dest-ip-address   dest-ipv6-address } filename [ ftp ftp-username ftp-password ] [ no-comparision ] [ reload ]</b>	Mandatory If the FTP option is not specified, TFTP is used for upgrade by default.

For example: In standalone mode, package and upgrade programs of all active boards via the FTP server 130.255.168.45.

```
Hostname#sysupdate package 130.255.168.45 sp9a-g-9.7.1.1(74)(R)-001.pkg FTP a a
```

#The device will prompt the following:

```
Downloading "sp9a-g-9.7.1.1(74)(R)-001.pkg" header...OK!
Checking "sp9a-g-9.7.1.1(74)(R)-001.pkg" header...OK!
```

image file version comparision:

```
-----
Component      Component version  File version
-----
Mpu 0          9.7.1.1(72)(integrity)  9.7.1.1(74)
```

The current-version of cards is greater than or equal to that in package.

NOTICE:input 'Yes' to upgrade all files in the package, 'No' to ignore the above component(s). (Yes|No)?y

```
Downloading "sp9a-g-9.7.1.1(74)(R)-001.pkg" :
#####
#####OK!
Download "sp9a-g-9.7.1.1(74)(R)-001.pkg" (146875569 Bytes) successfully!
Checking package file...OK!
Verify the image...valid
Writing file to
filesystem.....
.....OK!
Start backup ios to raw flash...[ 7557.521975] EXT4-fs error (device mmcblk0p2): ext4_mb_generate_buddy:755: group 2,
26114 clusters in bitmap, 32768 in gd

Apr 16 2021 12:30:00 switch MPU0 %SYS_UPDATE-RESULT-5:image : Mpu 0 write file to file-system successfully!OK
%Sysupdate image is in process, please wait...
Apr 16 2021 12:30:34 switch MPU0 %SYS_UPDATE-RESULT-5:image : Mpu 0 write file to backup file-system successfully!
Apr 16 2021 12:30:34 switch MPU0 %SYS_UPDATE-RESULT-5:image : Mpu 0 upgrade successfully!
%Sysupdate image finished.
Update bootloader start.
.....OK.
```

```
Downloading file to LPU3:
Apr 16 2021 12:30:41 switch MPU0 %SYS_UPDATE-RESULT-5:bootloader : Mpu 0 upgrade successfully!
```

```

#####
#####
#####OK!
Update bootloader of LPU3:.....successfully!
Downloading file to
LPU7:#####
#####
#####OK!
Update bootloader of LPU7:.....successfully!
Downloading file to
LPU9:#####
#####
#####OK!
Update bootloader of LPU9:.....successfully!
Downloading file to
SFU1:#####
#####
#####OK!
Update bootloader of SFU1:.....successfully!
%Sysupdate bootloader is in process, please wait...
%Sysupdate bootloader finished.
Update CMM of master MPU:Successfully!
Update CMM of LPU3:Successfully!
Update CMM of LPU7:Successfully!
Update CMM of LPU9:Successfully!
Update CMM of SFU1:Successfully!
%Sysupdate cmm is in process, please wait...
Apr 16 2021 12:31:21 switch MPU0 %SYS_UPDATE-RESULT-5:cmm : Mpu 0 upgrade successfully!
%Sysupdate cmm finished.
Writing file to filesystem...OK!

%Sysupdate devinfo is in process, please wait...
Apr 16 2021 12:31:22 switch MPU0 %SYS_UPDATE-RESULT-5:devinfo : Mpu 0 upgrade successfully!
%Sysupdate devinfo finished..
%Sysupdate pkgInfo is in process, please wait...
Apr 16 2021 12:31:24 switch MPU0 %SYS_UPDATE-RESULT-5:pkgInfo : Mpu 0 upgrade successfully!
%Sysupdate pkgInfo finished.

package sysupdate result information list:
-----
sp9a-g-9.7.1.1(74)(R).pck sysupdate result information list:
-----
Mpu 0 - upgrade successfully!

sz03-bootloader-M-cn6x-1.0.75.pck sysupdate result information list:
-----
Mpu 0 - upgrade successfully!
Sfu 1 - upgrade successfully!
Lpu 3 - upgrade successfully!
Lpu 7 - upgrade successfully!
Lpu 9 - upgrade successfully!

sz02-cmm-tim4-1.0.1.4.pck sysupdate result information list:
-----
Mpu 0 - upgrade successfully!
Sfu 1 - upgrade successfully!
Lpu 3 - upgrade successfully!
Lpu 7 - upgrade successfully!
Lpu 9 - upgrade successfully!

devInfo_sw_HIT_V2.122 sysupdate result information list:
-----
Mpu 0 - upgrade successfully!

pkg_info.txt sysupdate result information list:
-----
Mpu 0 - upgrade successfully!

```

#The above information indicates that the package files of all types of active boards have been successfully upgraded.

---

### Note

- For business board daughter card, it is only shown when the upgrade fails.
  - If the command option reload is added, the system prompts whether to save the configuration and whether to restart the device. However, usually the device is started after all programs are upgraded. Therefore, the reload option is not recommended.
- 

---

### Warning

- During the upgrade process, ensure that the device cannot be powered off, and avoid the unplugging of boards or rebooting operation; otherwise, the system may not boot up properly and files may be damaged.
- 

## 10.3 Example of typical configuration for software upgrade

### 10.3.1 Upgrade Package File

#### Network Requirements

- A PC acts as an FTP server, and Device acts as an FTP client. The network between the server and the device is normal.
- On the FTP server, set the user name of the device for logging in to the FTP server as admin and the password is admin; place the packaged program for upgrade under the FTP server directory to upgrade all software versions that the device supports for packaged upgrade.

#### Network Topology

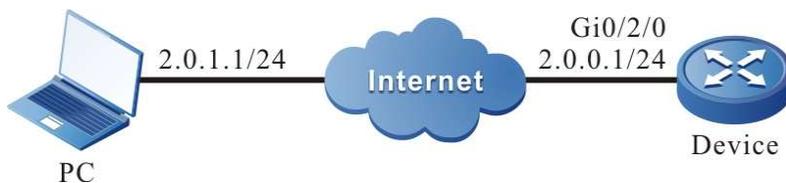


Figure 10-1 Network Topology for Packaged Upgrading of All Supported Software Versions

#### Configuration Steps

- 
- Step 1: Configure the FTP server and place the packaged program for upgrade in the directory of the FTP server. (Omitted)
- Step 2: Back up the device configuration file. (Omitted)
- Step 3: Configure the IP address of the interface to connect the device to the FTP server network. (Omitted)
- Step 4: Upgrade the packaged program.

#Use sysupdate to upgrade the packaged program.

```
Device#sysupdate package 2.0.1.1 sp9a-g-9.7.1.1(74)(R)-001.pkg ftp admin admin no-comparision
```

After the upgrade is completed, a list of upgrade results is printed out for the user to determine the upgrade results of programs included in the packaged upgrade file on the device.

package sysupdate result information list:

-----  
sp9a-g-9.7.1.1(74)(R).pck sysupdate result information list:

-----  
Mpu 0 - upgrade successfully!

sz03-bootloader-M-cn6x-1.0.75.pck sysupdate result information list:

-----  
Mpu 0 - upgrade successfully!  
Sfu 1 - upgrade successfully!  
Lpu 3 - upgrade successfully!  
Lpu 7 - upgrade successfully!  
Lpu 9 - upgrade successfully!

sz02-cmm-tim4-1.0.1.4.pck sysupdate result information list:

-----  
Mpu 0 - upgrade successfully!  
Sfu 1 - upgrade successfully!  
Lpu 3 - upgrade successfully!  
Lpu 7 - upgrade successfully!  
Lpu 9 - upgrade successfully!

devInfo\_sw\_HIT\_V2.122 sysupdate result information list:

-----  
Mpu 0 - upgrade successfully!

pkg\_info.txt sysupdate result information list:

-----  
Mpu 0 - upgrade successfully!

---

## Caution

- Please ensure that all boards are in position with their status in Start OK before packaged upgrade. Please do not unplug any board during the upgrade process to avoid upgrade abnormalities affecting the subsequent start-up of the board.

---

## Note

If you select the "no-comparison" parameter, the program will be upgraded directly using the version in the program without comparing the image versions. If this parameter is not selected, the image version will be compared, and if the image version in the packaged upgrade program is lower than or the same as the running version of the device, the device will prompt the user and wait for the user to confirm whether to upgrade the image program in the upgrade package.

Whether the user chooses to upgrade the program or not, it will not affect the upgrade of other upgrade files in the upgrade package. If the image file is the only file included in the upgrade package, the package upgrade ends if the user chooses not to upgrade.

- This command also allows you to add the "reload" parameter, which can reboot the device directly after the upgrade is completed.
- 

Step 5: Command to reboot the device

#Use the reload command to reboot the device.

```
Device#reload
Save current configuration to startup-config(Yes|No)?y
Please confirm system to reload(Yes|No)?y
```

It is up to the user to decide whether to save the configuration before rebooting.

---

## Note

- If the "reload" parameter is included in the upgrade command, this step is omitted.
- 

Step 6: Check the result.

#After the upgrade is completed and the device is rebooted, check the version information of the upgraded file in the program via the show package version command.

```
Device#show package version

package      :sp9a-g-9.7.1.1(74)(R)-001.pkg
image        :sp9a-g-9.7.1.1(74)(R).pck
bootloader   :sz03-bootloader-M-cn6x-1.0.75.pck
cmm          :sz02-cmm-tim4-1.0.1.4.pck
```

devinfo :devInfo\_sw\_HIT\_V2.122

#To verify if the update is successful, check the version number of each program via the show system verison brief co

Device#show system version brief

version information display:

Module	Online State	Name	BootLoader	IOS	CMM	PCB	CPLD	FPGA
Mpu 0	online Start Ok	SM89E-MPUC(V1)	1.0.74	9.7.1.1(74)(integrity)	1.0.1.4	002	106	106
Lpu 3	online Start Ok	SM89E-48XGEF-DB(V1)	1.0.74	9.7.1.1(74)(integrity)	1.0.1.4	002	104	/
Lpu 7	online Start Ok	SM89E-16QXGE-DB(V1)	1.0.74	9.7.1.1(74)(integrity)	1.0.1.4	002	105	/
Lpu 9	online Start Ok	SM89E-48GEF2XGEF-EA(V1)	1.0.74	9.7.1.1(74)(integrity)	1.0.1.4	002	105	/
Sfu 1	online Start Ok	SM89E-SFUD(V1)	1.0.74	9.7.1.1(74)(integrity)	1.0.1.4	001	102	/

## ! Caution

- The version of the upgrade file in the packaged upgrade program can be viewed via the show package version command, and the final upgrade result can be viewed via the show system verison brief command.

## 10.3.2 Full Upgrade of All Software Versions

### Network Requirements

- A PC acts as an FTP server, and the device Device acts as an FTP client. The network between the server and the device is normal.
- On the FTP server, set the user name of the device for logging in to the FTP server as admin and the password is admin; place the image program and bootloader program for upgrade under the FTP server directory to upgrade all software versions of the device.

### Network Topology



Figure 10-2 Network Topology for Upgrading of All Software Versions

### Configuration Steps

- Step 1: Configure the FTP server and place the image program and bootloader program for upgrade in the directory of the FTP server. (Omitted)
- Step 2: Back up the device configuration file. (Omitted)

Step 3: Configure the IP address of the interface to connect the device to the FTP server network.  
(Omitted)

Step 4: Upgrade the image program.

#Check if there is enough space left in the file system before upgrading the image program.

```
Device#filesystem  
Device(config-fs)#volume
```

#Use sysupdate to upgrade the image program of the MPU.

```
Device#sysupdate image mpu all 2.0.0.1 sp9a-g-9.7.1.1(74)(R).pck ftp admin admin
```

For information on image program upgrade process and whether the upgrade was successful, please refer to the relevant section on "Image Program Package Upgrade" in "Software Upgrade Configuration".

Step 5: Upgrade bootloader program.

#Use sysupdate to upgrade the bootloader program of the MPU.

```
Device#sysupdate bootloader mpu all 2.0.0.1 sz03-bootloader-M-cn6x-1.0.75.pck ftp admin admin
```

For information on bootloader program upgrade process and whether the upgrade was successful, please refer to the relevant section on "Bootloader Upgrade" in "Software Upgrade Configuration".

Step 6: Upgrade CMM program.

#Use sysupdate to upgrade the CMM program on all boards.

```
Device#sysupdate cmm all 2.0.0.1 sz02-cmm-tim4-1.0.1.4.pck ftp admin admin
```

For information on CMM program upgrade process and whether the upgrade was successful, please refer to the relevant sections on "CMM Upgrade" in "Software Upgrade Configuration".

Step 7: Upgrade FPGA program.

#Upgrade the FPGA program of the active/standby MPUs, CPOS, POS, E1 and other WAN daughter cards as needed, as shown in the following example: Use sysupdate to upgrade the FPGA program of all CPOS daughter cards on the device.

```
Device#sysupdate fpga all 2.0.0.1 pb035mpuc_fpv001_101.bin ftp admin admin
```

The upgrade command for the active/standby MPUs, POS, E1 and other WAN daughter cards shall follow suit, and only the file name needs to be changed. For information on FPGA program upgrade process and whether the upgrade was successful, please refer to the relevant section on "FPGA Upgrade" in "Software Upgrade Configuration".

---

---

## Note

- When upgrading FPGA, if the board type is not specified, the corresponding board will be searched automatically according to the FPGA program type for upgrading.
  - In general, FPGA program's update frequency is relatively low, so please confirm that the upgrade version is higher than the current running version of the system before upgrade. Please refer to step 10 below to check the current FPGA version of the system.
- 

### Step 8: Upgrade CPLD files

#Use sysupdate to upgrade the CPLD program on board.

```
Device#sysupdate cpld all 2.0.0.1 pb009pb009_nss12800_cpld_clv015.pck ftp admin admin
```

For information on CPLD program upgrade process and whether the upgrade was successful, please refer to the relevant section on "CPLD Program Package Upgrade" in "Software Upgrade Configuration".

### Step 9: Devinfo program upgrade

#Use sysupdate to upgrade the devinfo program of the MPU.

```
Device#sysupdate devinfo mpu all 2.0.0.1 devInfo(v2.2) ftp admin admin
```

For information on devinfo program upgrade process and whether the upgrade was successful, please refer to the relevant section on "Devinfo Upgrade" in "Software Upgrade Configuration".

### Step 10: Command to reboot the device.

#Use the **reload** command to reboot the device.

```
Device#reload
Save current configuration to startup-config(Yes|No)?y
Please confirm system to reload(Yes|No)?y
```

It is up to the user to decide whether to save the configuration before rebooting.

### Step 11: Check the result.

# After the upgrade is complete and the device is rebooted, verify that all versions have been updated by checking the version numbers of various programs.

#Verify that the image and bootloader programs of the active/standby MPU have been upgraded successfully.

```
Device#show system mpu
System Card Information(Mpu 0 - ONLINE)
-----
Type: SM89E-MPUC(V1)
Status: Start Ok
Last-Alarm: Normal
Card-Port-Num: 0
Card-SubSlot-Num: 0
```

Power-INTF-Status: Normal  
Power-Card-Status: On  
Serial No.:  
Description:  
Power-RT-Information:  
Voltage-In: 3.30 V  
Hardware-Information:  
PCB-Version: 002  
CPLD-Version: 106  
FPGA-Version: 106  
Software-Information:  
Bootloader-Version: 1.0.77  
Software-Version: 9.7.1.1(74)(integrity)  
Temperature-Information:  
Temperature-State:  
Switch-Temperature = 53 C  
Last-Alarm = Normal.  
InletAir-Temperature = 35 C  
Last-Alarm = Normal.  
CPU-On-Card-Information: < 1 CPUs>  
CPU-Idx: 00  
Status: Normal  
Core-Num: 0001  
Core-State:  
Core-Idx-00  
Core-Status: 0000  
Core-Utilization: 4%  
Temperature:  
Temperature-State:  
Temperature = 61 C  
Last-Alarm = Normal.  
MEM-On-Card-Information: <1 MEMs>  
MEM-Idx: 00  
MEM-State:  
BytesFree = 3632234496 bytes  
BytesAlloc = 526073856 bytes  
BlocksFree = 4 blocks  
BlocksAlloc = 3743 blocks  
MaxBlockSizeFree = 33554432 bytes  
SizeTotal = 4158308352 bytes  
DISK-On-Card-Information: <1 DISKs>  
DISK-Idx: 00  
Type: Flash  
Status: Online  
DISK-State:  
SizeTotal = 1890254848 bytes  
SizeFree = 1709191168 bytes  
FPGA-On-Card-Information: <1 FPGAs>  
FPGA-Idx: 00  
Status: Online  
Info-Struct:  
id = 0000  
version = 106  
CPLD-On-Card-Information: <1 CPLDs>  
CPLD-Idx: 00  
Info-Struct:  
version = 106  
CMM-Information:  
Software-Version: 1.0.1.4

-----  
STATISTICS: 1 IN, 0 OUT, 0 IERR, 0 OERR

System Card Information(Mpu 1 - ONLINE)

-----  
Type: SM89E-MPUC(V1)  
Status: Start Ok  
Last-Alarm: Normal  
Card-Port-Num: 0  
Card-SubSlot-Num: 0  
Power-INTF-Status: Normal

---

Power-Card-Status: On  
Serial No.:  
Description:  
Power-RT-Infomation:  
Voltage-In: 3.30 V  
Hardware-Information:  
PCB-Version: 002  
CPLD-Version: 106  
FPGA-Version: 106  
Software-Information:  
Bootloader-Version: 1.0.77  
Software-Version: 9.7.1.1(74)(integrity)  
Temperature-Information:  
Temperature-State:  
Switch-Temperature = 53 C  
Last-Alarm = Normal.  
InletAir-Temperature = 35 C  
Last-Alarm = Normal.  
CPU-On-Card-Information: <1 CPU>  
CPU-Idx: 00  
Status: Normal  
Core-Num: 0001  
Core-State:  
Core-Idx-00  
Core-Status: 0000  
Core-Utilization: 4%  
Temperature:  
Temperature-State:  
Temperature = 61 C  
Last-Alarm = Normal.  
MEM-On-Card-Information: <1 MEM>  
MEM-Idx: 00  
MEM-State:  
BytesFree = 3632234496 bytes  
BytesAlloc = 526073856 bytes  
BlocksFree = 4 blocks  
BlocksAlloc = 3743 blocks  
MaxBlockSizeFree = 33554432 bytes  
SizeTotal = 4158308352 bytes  
DISK-On-Card-Information: <1 DISK>  
DISK-Idx: 00  
Type: Flash  
Status: Online  
DISK-State:  
SizeTotal = 1890254848 bytes  
SizeFree = 1709191168 bytes  
FPGA-On-Card-Information: <1 FPGA>  
FPGA-Idx: 00  
Status: Online  
Info-Struct:  
id = 0000  
version = 106  
CPLD-On-Card-Information: <1 CPLD>  
CPLD-Idx: 00  
Info-Struct:  
version = 106  
CMM-Information:  
Software-Version: 1.0.1.4

-----  
STATISTICS: 1 IN, 0 OUT, 0 IERR, 0 OERR

Device#show devInfo  
vendor : HIT  
product Type : SWITCH  
devInfo version: V2.122



- 
- The interface of the device that can reach the FTP server by routing can be either a dc0 out-of-band management interface or a service interface.
  - There is no strict order for upgrading image and bootloader programs as mentioned above, but remember, you need to upgrade all programs before rebooting the whole device.
  - Before upgrading, you should ensure that there is enough space left in the flash file system of the active/standby MPU for saving the upgraded image files. If the remaining space on the device is insufficient, delete redundant files in the file system of the device; it is recommended to ensure that the remaining space of flash of the active/standby MPU is more than 170M before upgrading, otherwise the upgrade time may be extended.
  - If some programs have not been modified in the new released version, the unmodified programs can be left unupgraded.
  - If an exception occurs during the upgrade process, resulting in the unsuccessful upgrade of some boards, you can upgrade this part of the board separately later on.
- 

### 10.3.3 Upgrade bootloader using Console port.

#### Network Requirements

- A PC is directly connected to the device Console port.
- Use the Console port to upgrade the bootloader program of the active/standby MPU.

#### Network Topology

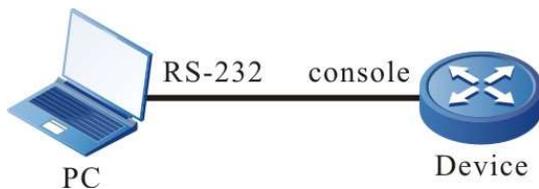


Figure 10-3 Using the Console Port to Upgrade the bootloader Program

#### Configuration Steps

Step 1: A PC is properly connected to the Console port of the device. (Omitted)

Step 2: Open the bootloader screen.

Press and hold "ctrl+c" to open the bootloader screen when the device has just booted up and printed "Press ctrl+c to enter bootloader mode: 0".

Step 3: Set the transfer rate to 115200bps to speed up the upgrade.

```
bootloader#srata 115200
```

#After setting the transfer rate of Console port under bootloader, the transfer rate of HyperTerminal should be set to 115200bps as well.

---

Step 4: Upgrade the bootloader version in the bootloader environment.

```
bootloader#mupdate bootloader
```

#Enter the command "mupdate bootloader" to transfer the bootloader file saved on the PC using ymodem.

#Check the result.

#The following message will be printed on the bootloader screen after the upgrade is completed.

```
bootloader# mupdate bootloader
Download bootloader start...
run command=loady
## Ready for binary (ymodem) download to 0x20000000 at 115200 bps...
C
Transferring sz03-bootloader-M-cn6x-1.0.75.pck, errors 0...
 100% 1911 KB   3 KB/sec  00:08:17   0 Errors

## Total Size   = 0x001ddd94 = 1957268 Bytes
Download bootloader OK.
bootloader image check:
..... done
Un-Protected 8 sectors

..... done
Erased 8 sectors
run command=cp.b 200000f8 0x17c00000 0xeb020
Copy to Flash... done
..... done
Protected 8 sectors
Update bootloader OK..
```

Step 5: Check the result.

#Rebooting the device after the upgrade is complete, and the system will print that the system is loaded guided by the new bootloader.

```
Bootloader 1.0.75 (Build time: Apr 09 2021 - 10:38:53)
```

```
Warm boot from master sector
```

```
Press ctrl+c to enter bootloader mode: 0
```

---

### Note

- Since upgrading the bootloader program via Console port is more complicated and time-consuming, it is usually recommended to use TFTP to upgrade the bootloader program, and use the Console port to upgrade the bootloader program only when the conditions of the former are not met.
- After the upgrade is complete, exit the bootloader with the "reset" command and let the new bootloader program guide the image program to load.
- When upgrading the bootloader program, if the default baud rate of the Console port is modified, the Console port rate of the device is automatically restored to 9600bps when loading the image package, and the rate of the HyperTerminal needs to be modified as well.

# 11 Bootloader

---

## 11.1 Overview

In embedded systems, the bootloader program runs before the OS kernel runs and is used to initialize hardware devices (including Console ports, Ethernet interfaces, flash, etc.), establish memory space mapping, thus bring the system's hardware and software environment to a suitable state in order to prepare the correct environment for the eventual boot of the OS kernel. In an embedded system, there is usually no firmware program like BIOS, and the loading and booting task of the whole system is done by bootloader.

The bootloader system mainly contains the following functions:

- Set startup parameters to load IOS via network device or internal flash memory device
- Upgrade bootloader program.
- Back up bootloader program.

## 11.2 bootloader Function Configuration

Table 11-1 bootloader Function Configuration List

Configuration Task	
Enter the bootloader configuration mode	Enter the bootloader configuration mode upon startup
Set bootloader startup parameters	Set bootloader startup parameters to boot the image program in flash.

Configuration Task	
Configure the bootloader to manage the Ethernet port IP address.	Configure the bootloader to manage the Ethernet port IP address.
Upgrade bootloader program.	Upgrade bootloader program.

### 11.2.1 Preparation for bootloader function configuration

Before starting the bootloader configuration, you need to set up the local configuration environment. Connect the serial port of the host (or terminal) to the Console port of the device through the configuration cable, and the configuration of the communication parameters of the host (or terminal) and the default configuration of the Console port of the device need to be consistent. The default configuration of the Console port on the device is:

- Transmission rate: 9600bps
- Flow control mode: None
- Calibration method: None
- Stop Bit: 1Bit
- Data bits: 8Bit

### 11.2.2 Enter the bootloader configuration mode

#### Configuration Condition

None

#### Enter the bootloader configuration mode

Table 11-2 Entering the bootloader Configuration Mode

Step	Command	Description
Enter the bootloader configuration mode	None	Mandatory After the device is powered on, press and

Step	Command	Description
		hold "ctrl+c" to enter the bootloader configuration mode; after entering, the prompt message is: "bootloader#"

### Note

- After entering the bootloader configuration mode, you can perform the functions provided by the bootloader mode.

## 11.2.3 Set bootloader startup parameters

### Configuration Condition

None

### Set Bootloader Startup Parameters

Table 11-3 Setting the bootloader Startup Parameters

Step	Command	Description
Enter the bootloader configuration mode	None	Mandatory After the device is powered on, press and hold "ctrl+c" to enter the bootloader configuration mode; after entering, the prompt message is: "bootloader #"
Set IOS startup parameters under bootloader	<b>change</b> <i>index[0~3]</i> <b>dc0</b> <i>filename local-ip-addr</i>	Mandatory The first line of the command is the network

Step	Command	Description
	<pre> host-ip-addr [ gatewayip ] [ netmask ]  change index[0~3] flash0 filename </pre>	<p>startup configuration parameters, if you upgrade across network segments, you need to add the gateway and mask.</p> <p>The second line of the command is the startup configuration parameters for flash storage device.</p>

### Note

- The bootloader program of the domestic switch currently can set startup parameters to boot the image program over network.

## 11.2.4 Upgrade bootloader program.

### Configuration Condition

None

### Upgrade bootloader program.

Table 11-4 Upgrading bootloader Program

Step	Command	Description
Enter the bootloader configuration mode	None	<p>Mandatory</p> <p>After the device is powered on, press and hold "ctrl+c" to enter the bootloader configuration mode; after entering, the</p>

Step	Command	Description
		prompt message is: "bootloader#"
Start tftp server on the PC.		Mandatory  Copy the new bootloader version used for the upgrade to the root directory of tftp for the device to download the version file via tftp.
Upgrade bootloader program.	<b>update bootloader</b> <i>filename dc0 local-ip-addr host-ip-addr [gatewayip] [netmask]</i>	Mandatory  Upgrade the PCK file of bootloader via tftp server
	<b>mupdate bootloader</b>	Optional  For transmission via ymodem, refer to the command manual for details.
Back up bootloader program.	<b>bootloaderbak</b>	Optional

---

## Note

- The bootloader system program adopts a dual bootloader backup mode, i.e. it has both the main bootloader program and the backup bootloader program, using the upgrade command can only upgrade the program version of the main bootloader, while the backup bootloader program will remain unchanged.
  - After upgrading the bootloader system program, use the command **reset** or power off and reboot the device to use the latest bootloader system program.
  - When the system is loaded successfully, you can upgrade it with the **sysupdate**
-

---

command.

---

## 11.2.5 bootloader Monitoring and Maintaining

Table 11-5 bootloader Monitoring and Maintaining

Command	Description
<b>version</b>	Display the bootloader program version number.
<b>print index[0~4]</b>	Display startup parameters information specified by index.
<b>boot index[0~4]</b>	Load the startup parameters information specified by index.
<b>clear index[0~3]</b>	Clear the startup parameters information specified by index.
<b>grate</b>	Obtain data on the speed rate of the current serial port.
<b>Srate ratenum</b>	Obtain data on the speed rate of the current serial port, the value of which is taken as 9600 or 115200.

## 11.3 bootloader Typical Configuration Example

### 11.3.1 Configure the bootloader to start the Image program via the network.

#### Network Requirements

- A PC acts as a TFTP server, and Device acts as a TFTP client. The network between the server and the device is normal.
- On the TFTP server, place the image program and bootloader program that need to be upgraded in the TFTP server directory.

## Network Topology

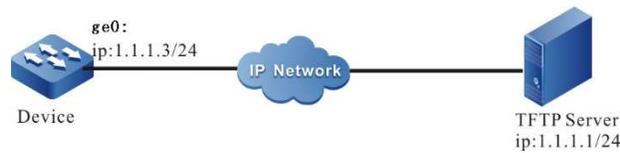


Figure 11-1 Configuring the bootloader to Boot the Image Program via the Network

### Configuration Steps

- Step 1: Configure TFTP server and place the image program in the directory of the TFTP server. (Omitted)
- Step 2: After the device is powered on, press and hold "ctrl+c" to enter the bootloader configuration mode.
- Step 3: Configure the startup line parameters to start the Image program via the network.

For instance,

```
bootloader#change 0 dc0      sp9b-g-9.7.1.1(68)(R).pck 1.1.1.3 1.1.1.1
bootloader#boot 0
```

---

### Note

- Connect the first port of the device to the tftp server.
  - After setting the startup information, the device can communicate with the tftp server normally before performing boot.
- 

# 12 PoE Management

---

## 12.1 Overview

The existing Ethernet, with its basic structure of Cat.5 cabling unchanged, not only transmits data signals for IP-based terminals (such as IP phones, WLAN access points, and network cameras), but also provides the DC power supply for the devices. This technology is called Power over Ethernet (PoE). The PoE technology ensures not only the security of existing structured cabling but also normal operation of the existing network, greatly reducing the cost.

PoE is also called Power over LAN (PoL) or Active Ethernet. It is the latest standard specification for making use of existing standard Ethernet transmission cable to transmit data and provide power. It is compatible with the existing Ethernet systems and users. IEEE 802.3af and IEEE802.3at are the technical standards that PoE must comply with. IEEE802.3af is the basic standard of the PoE technology. It is based on the IEEE 802.3, and the standards related to direct power supply through network cables are added. It is an extension of the existing Ethernet standards. IEEE802.3at is an extension based on the IEEE802.3af.

According to the definition of the IEEE802.3af standard, a complete PoE power supply system consists of two types of devices: Power Sourcing Equipment (PSE) and Power Device (PD).

- PSE: It provides power to other devices.

**12.1.1** PD (Power Device): Devices that receive power. The power of the devices is usually not large.

### PSE/PD Interface Specifications

For the 10BASE-T and 100BASE-TX networks, IEEE802.3af defines Power Interfaces (PIs), which are interfaces between PSE/PD and network cables. Currently, it has defined two power supply modes, Alternative A (xsignal wire pairs 1, 2, 3 and 6) and Alternative B (signal wire pairs 4, 5, 7, and 8). The following is a description of the two power supply modes:

#### 1. Power supply through signal wire pairs (Alternative A)

As shown in the following figure, a PSE can supply power to a PD through signal wire pairs. Because DC and data frequency does not interfere with each other, electric current and data can be transmitted through the same wire pair. For electric cables, this is a kind of "multiplexing". Wires 1 and 2 are connected to form a positive (or negative) polarity, and wires 3 and 6 are connected to form a negative (or positive) polarity.

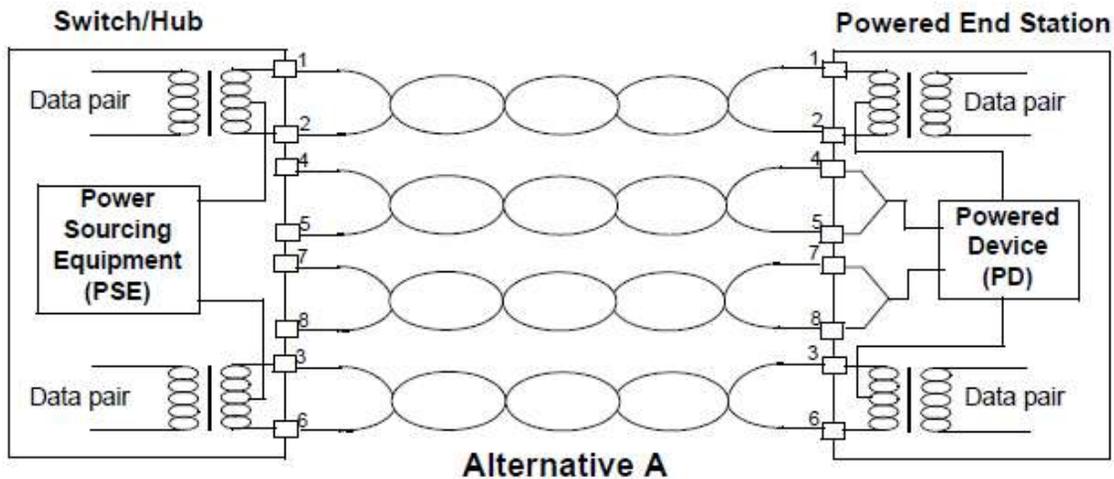


Figure 12-1 Alternative A Power Supply Mode with 10BASE-T and 100BASE-TX

## 2. Power supply through idle wire pairs (Alternative B)

As shown in the following figure, a PSE can supply power to a PD through idle wire pairs. Wires 4 and 5 are connected to form a positive polarity, and wires 7 and 8 are connected to form a negative polarity.

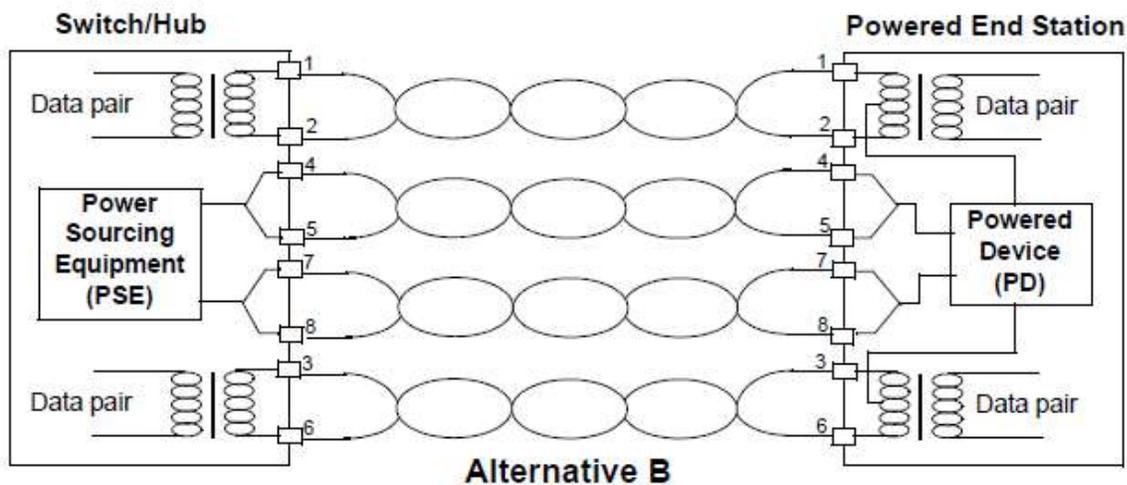


Figure 12-2 Alternative B Power Supply Mode with 10BASE-T and 100BASE-TX

According to IEEE802.3af, standard PDs must support both power supply through signal wire pairs and power supply through idle wire pairs, while PSEs need only support either of the two modes.

### 12.1.2 PoE Power Supply Process

If a PSE is installed in a network, the PoE Ethernet power supply process is as follows:

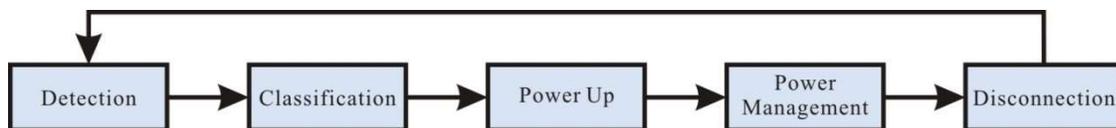


Figure 3-4 PSE Power Supply Process

- **Detection:** After a network device is connected to a PSE, the PSE first detects whether the device is a PD to ensure that the current is not supplied to non-PDs because supplying power to a device that is not a PD may damage the device. The PSE detects the resistance capacitance between the power output wire pairs to determine whether PDs exist. The PSE proceeds to the next step only after it detects PDs.
- **Classification:** After detecting PDs, the PSE classifies the PDs. It determines power grade of PDs by detecting power output current. During the power supply process, classification is optional.
- **Power Up:** Within a startup period which is configurable (usually less than 15 us), the PSE starts to provides low power voltage to PDs and gradually increases the power voltage to 48 V DC.
- **Power Management:** The PSE provides stable and reliable 48 V DC power for PDs. Once the PSE starts to supply power, it continuously detects PD current inputs. If the current consumption of a PD drops under the minimum value owing to various causes, such as the PD is disconnected, the PD encounters power consumption overload or short circuit, and the power load exceeds the PSE power supply load, the PSE regards the PD as not in position or abnormal. In this case, the PSE stops providing power to the PD.
- **Disconnection:** The PSE detects the current of PDs to determine whether PDs are disconnected. If a PD is disconnected, the PSE stop supplying power to the PD quickly (usually within 300 to 400 ms), and then the PSE returns to the Detection status.

## 12.2 PoE Function Configuration

Table 12-1 PoE Function Configuration List

Configuration Task	
PoE Basic Function Configuration	Enable the Global PoE Function
	Enable the Interface PoE Function

Configuration Task	
	Enable the Forced Power Supply Function of an Interface
	Enable the Auto Power Supply Function of an Interface
Configure the PoE Power	Configure the Total Power of PoE
	Configure the Protection Power of PoE
	Configure the Maximum Output Power Limit Mode of an Interface
	Configure the Maximum Output Power of an Interface
Configure Power Supply Priorities	Configure a PoE Power Management Mode
	Configure the Power Supply Priority of an Interface
Configure PD Power-up and Power-down Parameters	Configure Interface PD Detection Mode
	Configure Interface Classification Mode
	Configure Interface Power-up Inrush Current Mode
	Configure Interface Power Supply Wire Pairs
	Configure Interface Power Failure Detection Mode
Configure the Abnormality Recovery Function	Configure the Time for Recovery from a Power Supply Abnormality of an Interface
	Restart the PoE Power Supply

Configuration Task	
Configure PoE Power Alarm Function	Configure PoE Power Alarm Threshold

### 12.2.1 PoE Basic Function Configuration

The PoE function is controlled by configuring global PoE and interface PoE, that is, the PoE function can be used only when the global PoE and interface PoE are both enabled. If you run the command for disabling the global PoE, the PoE functions of all interfaces are disabled. If you run the command for disabling the interface PoE function, you can choose to disable the PoE function of some interfaces. The interface PoE function is a standard power supply mode, while the interface forced power supply function is a special power supply mode. You can select only one mode at a time. However, both of the two modes are valid only after the global PoE function is enabled.

#### Configuration Condition

None

#### Enable the Global PoE Function

Table 12-2 Enabling the Global PoE Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable the Global PoE Function	<b>power enable</b>	Optional By default, the global PoE function is enabled.

#### Enable the Interface PoE Function

Table 12-3 Enabling the Interface PoE Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Enable the Global PoE Function	<b>power enable</b>	Optional By default, the global PoE function is enabled.
Enter the L2/L3 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	-
Enable the Interface PoE Function	<b>power enable</b>	Optional By default, the interface PoE function is enabled.

### Enable the Forced Power Supply Function of an Interface

Table 12-4 Enabling the Forced Power Supply Function of an Interface

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable the Global PoE Function	<b>power enable</b>	Optional By default, the global PoE function is enabled.
Enter the L2/L3 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	-
Enable the Forced Power Supply Function of an Interface	<b>power force { always   once }</b>	Mandatory By default, the forced power supply function of an interface is disabled.

---

 **Note**

Forced power supply is a special power supply mode, which does not require enabling the interface PoE function.

---

### Enable the Auto Power Supply Function of an Interface

Table 12-5 Enabling the Auto Power Supply Function of an Interface

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable the Global PoE Function	<b>power enable</b>	Optional By default, the global PoE function is enabled.
Enter the L2/L3 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	-
Enable the Auto Power Supply Function of an Interface	<b>power auto-enable</b>	Mandatory By default, the auto power supply function of an interface is disabled.

---

 **Note**

The auto-power supply function of an interface works only in manual power management mode.

---

## 12.2.2 Configure the PoE Power

### Configuration Condition

Before configuring the PoE power, ensure that:

- Enable the Global PoE Function.
- Enable the Interface PoE Function.

### Configure the Total Power of PoE

By configuring the total power of PoE, you can limit maximum output power of the device. If the total power required by all PDs exceeds the configured total power, power supply to some PDs is stopped according to the current power supply priority mode.

Table 12- 6 Configuring the Total Power of PoE

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the Total Power of PoE	<b>power total-power { all   system-id { all   subsystem-id } } power-value</b>	Optional By default, the total power is the maximum total power that the device power supply can provide.

### Configure the Protection Power of PoE

When a PD is normally powered, the consumed power fluctuates within a certain range. To prevent PD power-off owing to power fluctuation, part of power is reserved from the total power of the device to act as the protection power. When the consumed power of the PD increases, the increased part is allocated from the protection power.

Protection power may also be allocated as normal power supply. When the available power is insufficient for providing power to newly connected PDs, if the available power of the device and the protection power is equal to or larger than the maximum output power of the interface of the new PD, sufficient power is allocated from the protection power to the new PD.

Table 12-6 Configuring the Protection Power of PoE

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the Protection Power of PoE	<b>power guard-band { all   system-id { all   subsystem-id } } guard-band-value</b>	Optional By default, the protection power of the power supply is 40.0 watt.

### Configure the Maximum Output Power Limit Mode of an Interface

The maximum output power of an interface is determined by the PD classification type. You can also customize the maximum output power of an interface.

Table 12-7 Configuring the Maximum Output Power Limit Mode of an Interface

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the L2/L3 Ethernet interface configuration mode.	<b>interface interface-name</b>	-
Configure the Maximum Output Power Limit Mode of an Interface	<b>power threshold-mode { classification   user }</b>	Optional By default, the maximum output power limit mode is the user customization mode.

### Configure the Maximum Output Power of an Interface

You can limit the maximum power that a PSE can supply to a PD through an interface. If the power required by a PD exceeds the maximum output power of the interface, the PSE stops power supply to it.

Table 12-8 Configuring the Maximum Output Power of an Interface

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the L2/L3 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	-
Configure the maximum output power limit mode to the user customization mode.	<b>power threshold-mode user</b>	Mandatory By default, the maximum output power limit mode is the user customization mode.
Configure the Maximum Output Power of an Interface	<b>power port-max-power</b> <i>max-power-value</i>	Optional By default, the maximum output power is 30.0 watt.

### 12.2.3 Configure Power Supply Priorities

With the power supply priority function, if the total power of a PSE is insufficient for powering all PDs, key PDs have the priority to obtain power. Through this function, you can configure the mode in which key PDs are powered.

#### Configuration Condition

Before configuring power supply priorities, ensure that:

- Enable the Global PoE Function.
- Enable the Interface PoE Function.

#### Configure a PoE Power Management Mode

Table 9-10 Configuring a PoE Power Management Mode

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Configure a PoE Power Management Mode	<b>power manage</b> { <b>all</b>   <i>system-id</i> { <b>all</b>   <i>subsystem-id</i> } } { <b>dynamic-fifs</b>   <b>dynamic-priority</b>   <b>static-fifs</b>   <b>static-priority</b> }	Optional  The default power management mode is the dynamic First In First Served (FIFS).

### Configure the Power Supply Priority of an Interface

If the PoE power management mode is dynamic priority mode, when the power supply of PSE is insufficient, the system will prioritize power supply to the PD with a higher interface power supply priority. If the interface power supply priority is the same, then priority is given to the PD with the smaller interface number.

Table 12-11 Configuration of Interface Power Supply Priority

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure a PoE Power Management Mode to Dynamic Priority Mode	<b>power manage</b> { <b>all</b>   <i>system-id</i> { <b>all</b>   <i>subsystem-id</i> } } <b>dynamic-priority</b>	Mandatory  The default power management mode is the dynamic First In First Served (FIFS).
Enter the L2/L3 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	-
Configure the Power Supply Priority of an Interface	<b>power priority</b> { <b>critical</b>   <b>high</b>   <b>medium</b>   <b>low</b> }	Optional  By default, the power supply priority is low.

## 12.2.4 Configure PD Power-up and Power-down Parameters

The PoE power-up process is divided into several steps:

1. Detection: PSE detects the presence of PD.
2. Classification: PSE classifies the PD and determines the PD power consumption. This step is optional.
3. Power-Up: PSE supplies power to PD.

The parameters of the above steps can be adjusted to power different types of PDs.

### Configuration Condition

Before configuring the PD power-up parameters, first complete the following tasks:

- Enable the Global PoE Function.
- Enable the Interface PoE Function.

### Configure Interface PD Detection Mode

When an interface PoE function is enabled, the PSE detects the resistance capacitance between the power output wire pairs to determine whether PDs exist. The standard detection mode can only detect PDs that comply with IEEE802.3af and IEEE802.3at standards. The standard defines PD and non-PD, however, there is another device with a resistance and capacitance value between PD and non-PD, and the compatibility mode is used to detect this type of device.

Table 12-12 Configuring Interface PD Detection Mode

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the L2/L3 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	-
Configure Interface PD Detection Mode	<b>power detect-mode</b> { <b>compatible</b>   <b>standard</b> }	Optional By default, PD detection mode is standard mode.

### Configure Interface Classification Mode

After an interface PoE function is enabled, the PSE determines the power level of the PD by detecting the power supply output current. Corresponding power is assigned to the PD according to the power level of the PD. PD classification is an optional step in the overall power-up process and can be configured to skip this step by going to unclassified mode.

Table 12-13 Configuring Interface Classification Mode

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the L2/L3 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	-
Configure Interface Classification Mode	<b>power class-mode</b> { <b>standard</b>   <b>never</b> }	Optional By default, it is unclassified in the classification mode.

### Note

Some non-standard PDs may not support classification, in which case the default classification for the PD is class0 and the maximum output power of the interface is 15.4 Watts.

### Configure Interface Power-up Inrush Current Mode

The PoE standard regulates the inrush current when powering up the PD. This parameter is related to the PSE, the (parasitic) capacitance of the PD, and the PD power. For some PDs that do or do not meet the specification, the required onrush current may vary and the appropriate onrush current mode needs to be configured for the different PDs.

Table 12-14 Configuring Interface Power-up Inrush Current Mode

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Enter the L2/L3 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	-
Configure Interface Power-up Inrush Current Mode	<b>power power-up-mode</b> { <b>802.3af</b>   <b>high</b>   <b>Pre-802.3at</b>   <b>802.3at</b> }	Optional By default, the power-on inrush current mode is high inrush current.

### Configure Interface Power Supply Wire Pairs

The PoE standard regulates two power supply modes, idle wire pairs and data wire pairs. Standard PDs must support both power supply through signal wire pairs and power supply through idle wire pairs, while PSEs need only support either of the two modes.

Table 12-15 Configuring the Interface Power Supply Wire Pairs Mode

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the L2/L3 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	-
Configure Interface Power Supply Wire Pairs Mode	<b>power power-pair</b> { <b>pair-A</b>   <b>pair-B</b> }	Optional By default, the power supply wire pairs mode is data wire pairs.

### Note

PSE devices only support the data wire pairs power supply mode.

## Configure Interface Power Failure Detection Mode

PSE switches can provide different power failure detection modes depending on the type of current supplied DC or AC.

Table 12- 16 Configuring Interface Power Failure Detection Mode

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the L2/L3 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	-
Configure Interface Power Failure Detection Mode	<b>power disconnect{ ac   dc }</b>	Optional By default, the power failure detection mode is AC.

---

### Note

The PoE function of the PSE device is integrated into the switch, and the interface power failure detection mode on the device is AC mode by default.

---

## 12.2.5 Configure the Abnormality Recovery Function

When there is a PoE power supply abnormality, the abnormality recovery function is supported, including automatic recovery and manual recovery.

### Configuration Condition

Before configuring the abnormality recovery function, ensure that:

- Enable the Global PoE Function.
- Enable the Interface PoE Function.

## Configure the Time for Recovery from a Power Supply Abnormality of an Interface

If a PSE detects abnormal power supply status of an interface while powering PDs, it automatically disables the PoE function of the interface. After the time for recovery from a power supply abnormality elapsed, it enables the PoE function again, and tries to supply power to the PD of the interface.

Table 12-16 Configuring the Time for Recovery from a Power Supply Abnormality of an Interface

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the L2/L3 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	-
Configure the Time for Recovery from a Power Supply Abnormality of an Interface	<b>power recover-time</b> <i>time-value</i>	Optional By default, the recovery time for a power supply abnormality is 0 minutes, indicating immediate recovery after the abnormality.

## Restart the PoE Power Supply

When a PoE power supply abnormality occurs or the PoE power supply is abnormal, you can manually hot restart the PoE power supply to try to recover from the abnormal status.

Table 12-17 Configuring the Time for Recovery from a Power Supply Abnormality of an Interface

Step	Command	Description
Restart the PoE Power Supply	<b>power reload</b> { <b>all</b>   <i>system-id</i> }	Mandatory

---

 **Note**

During the power reboot process, the module will be initialized. You should avoid repeatedly operating power reload and wait until the power reboot is completed before executing it.

---

## 12.2.6 Configure PoE Power Alarm Threshold

### Configuration Condition

Before configuring the PoE power, ensure that:

- Enable the Global PoE Function.
- Enable the Interface PoE Function.

### Configure PoE Power Alarm Threshold

When PoE power utilization reaches or falls below the set power threshold, Trap alarms are sent.

Table 12-18 Configuring PoE Power Alarm Threshold

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure PoE Power Alarm Threshold	<b>power alarm-threshold</b> { <b>all</b>   <i>system-id</i> { <b>all</b>   <i>subsystem-id</i> } } <i>threshold-value</i>	Optional By default, the alarm threshold for power supply is 99%.

## 12.2.7 PoE Monitoring and Maintaining

Table 12-19 PoE Monitoring and Maintaining

Command	Description
<b>show power</b> { <b>manage</b>   <b>summary</b>   <b>configure interface</b> <i>interface-name</i>   <b>detect interface</b> <i>interface-name</i>   <b>pd-</b> <b>status interface</b> <i>interface-name</i>   <b>system-to-port</b> [ <i>system-id</i> ]   <b>version</b> }	Display PoE configuration, power supply status and port correspondence information, and system-to-port is only available in VST mode.

# 13 PDI

---

## 13.1 Overview

PDI: PD Inspection, refers to a way to detect whether the PD terminal is active, if the PD is not detected, it is considered abnormal and the POE is notified to restart the power supply.

The PDI function is controlled by configuring interface PDI, that is, the PDI function can be used only when the interface PDI is enabled.

## 13.2 Configure PDI Basic Functions

Table 13-1 Enabling Interface PDI Function

Step	Command	Description
Enter the L2/L3 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	-
Enable interface PDI function.	<b>pd enable</b>	Mandatory

Step	Command	Description
		By default, the interface PDI function is not enabled.

### 13.3 Configure the ARP packet delivery interval.

Table 13-2 Configuring the Interface ARP Packet Delivery Interval

Step	Command	Description
Enter the L2/L3 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	-
Configure the interface ARP packet delivery interval.	<b>pdi inspection-interval</b>	Optional By default, the interface arp packet delivery interval is 3s.

### 13.4 Configure the number of retries for ARP packet delivery.

Table 13-3 Configuring the Number of Retries for ARP Packet Delivery

Step	Command	Description
Enter the L2/L3 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	-
Configure the number of retries for ARP packet delivery of an interface.	<b>pdi inspection-retry</b>	Optional By default, the number of retries for ARP packet delivery of an interface is 3.

## 13.5 Configuring IP Inspection Table Entries

Table 13-4 Configuring IP Inspection Table Entries

Step	Command	Description
Enter the L2/L3 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	-
Configure ip detection table entries for PD.	<b>pdi ip-address</b>	Optional

## 13.6 PDI monitoring and maintaining

Table 13-5 1PDI Monitoring and Maintaining

Command	Description
<b>show pdi</b> {   <b>brief</b>   <b>interface</b> <i>interface-name</i>   <b>ip-entry ip-entry interface</b> <i>interface-name</i>   <b>statistic statistic interface</b> <i>interface-name</i> }	Display PDI global structure, port summary information and detailed information, etc.

# 14 LUM

## 14.1 Overview

***LUM:** Local User Manager, is a local user database used to provide local authentication for aaa.*

***RBAC:** Role Based Access Control, enables privileges to be granted to roles by establishing the association "Permissions <-> Roles", and assigns roles to users by establishing the association "Roles <-> Users", so that users can obtain the privileges of the corresponding roles. The basic idea of RBAC is to assign roles to users that define which system functions and resource objects they are allowed to operate.*

Since permissions and users are separated, RBAC has the following advantages:

- Administrators do not need to specify permissions for users one by one, but only need to pre-define roles with corresponding permissions, and then assign the roles to users. Therefore, RBAC is more adaptable to user changes and increases the flexibility of user privilege assignment.
- Since the relationship between roles and users often changes, but the relationship between roles and permissions is relatively stable, using this stable association can reduce the complexity of user authorization management and reduce management overhead.

**Role:** A collection of rules.

**Rule:** permit/deny permissions for commands of specific feature or all features.

**Feature:** Module.

## 14.2 LUM Function Configuration

Table 14-1 LUM Function Configuration List

Configuration Task	
Configure user roles	Configure user roles

Configuration Task	
Configure administrator program	Configure administrator
	Configure administrator user group
Configure access user program	Configure access user
	Configure user group

### 14.2.1 Configure Access

By default, there are four types of roles: Security-admin, Network-admin, Audit-admin and Network-operator, and the permissions of these four roles cannot be modified.

Custom role permissions are a subset of the network administrator role permissions. Module permissions that have been assigned to the Security-admin, or the Audit-admin cannot be configured. Please see the following table for specific permissions.

Table 14-2 Permissions of Individual User Role

	Logging	History	User management and user authentication	Other modules
Public Elective	NO	NO	Change your own password	Show running, exit, etc.
Security Administrator	View Operation log and related configuration commands	History configuration and operation	OK	lai module, line, service, AAA
Audit Administrator	View data log and configuration commands	NO	NO	NO

network administrator	All commands other than operation log and data log	Histroy configuration and operation	NO	OK
Network Operator	All show commands within the privileges of network operator	show command	NO	All show commands within the privileges of network operator

By default, the user does not have the role attributes configured. When the role attribute is in effect, the user level is no longer in effect, and the role replaces the user level as the basic criterion for command authorization: users have different command execution rights depending on their respective roles.

### Configuration Condition

None

### Configure user roles

Table 14-3 Configuring User Roles

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Create user roles and enter user role mode at the same time	<b>role <i>role-name</i></b>	Mandatory  By default, there are four types of roles: Security-admin, Network-admin, Audit-admin and Network-operator, and the permissions of these four roles cannot be modified.

Step	Command	Description
Create a rule for the user role	<b>rule</b> <i>number</i> { <b>deny</b>   <b>permit</b> } <b>feature</b> { <b>all</b>   <i>feature-name</i> }	By default, no rules are defined for newly created user roles, i.e., the current user role does not have any privileges.  The rule modification does not take effect for users who are currently online, but for users who log in later to use the rule for that role.  Rules with smaller rule IDs have higher priority.

## 14.2.2 Configure local users

Local users are those stored on the device: including local administrators and local access users. It only takes effect when local authentication mode is used. A local user is specified as an administrator or an access user when it is created.

### Configuration Condition

None

### Configure Local Administrator User

Table 14-4 Configuring Administrator

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Create an user administrator and enter the user administrator mode	<b>local-user</b> <i>user-name</i> class manager	Mandatory.  By default, no administrator user is configured.

## Configure Local Access User

Table 14-5 Configuring Access User

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Create access user and enter access user mode at the same time.	<b>local-user</b> <i>user-name</i> <b>class</b> <b>network</b>	Mandatory. By default, no access user is configured.

### 14.2.3 Configure administrator user attributes

An administrator is the user who logs into the device.

The following configuration restrictions and guidelines apply when configuring the attributes of local administrator user:

- If the user authorizes the role upon login through AAA, whether the user can execute commands after logging in to the device is determined by the role, and if the role is not authorized by AAA when the user logs in, whether the user can execute commands after logging in to the device is determined by the user level.
- For SSH users, when using public key authentication, if the authentication method for logging in to the device is not configured in the user line view, the commands available to them are based on the user role or user level (user role has higher priority than user level) set in the local administrator user view with the same name as the SSH user. For more information about user roles, please refer to "Configuring Roles" in the "LUM Configuration Guide".
- The attribute regarding the maximum number of password attempts for users can be configured in both local administrator user view and administrator user group view, and the order of priority for configuration is: local administrator user view -> administrator user group view, in descending order.
- The user password lifetime attribute can be configured in local administrator user view, administrator user group view and global view, and the order of priority for configuration is: local administrator user view --> administrator user group view --> global view, in descending order.

#### Configuration Condition

None

### Configure administrator user attributes

Table 14-6 Configuring Administrator

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Create an user administrator and enter the user administrator mode	<b>local-user</b> <i>user-name</i> class manager	Mandatory. By default, no administrator user is created.
Configure the administrator user password.	<b>password 0</b> <i>password</i>	Mandatory. By default, a user does not have a password.
Set the types of servers that users can use.	<b>service-type { ssh   telnet   console   ftp   web }</b>	Mandatory. By default, a user does not support any service-type.
Set the user role for the local user.	<b>user-rol</b> <i>role-name</i>	Optional. <b>By default, no administrator role is configured .</b> The administrator role has higher priority over the administrator level, that is, when the role for the administrator user is configured, the administrator privileges are subject to the administrator role.

Step	Command	Description
Set the user group for the administrator user.	<b>group</b> <i>group-name</i>	Optional. By default, no user group is configured.
Configure the authorized level of login user.	<b>privilege</b> <i>privilege-level-number</i>	Optional. By default, the authorized level is 1.
Configure the commands to be executed automatically by the user.	<b>autocommand</b> <i>command-line</i>	Optional. <b>By default, users do not have commands that are configured to be executed automatically.</b>
Configure options for users to automatically execute commands.	<b>autocommand-option</b> { <b>nohangup</b> [ <b>delay</b> <i>delay-time-number</i> ]   <b>delay</b> <i>delay-time-number</i> [ <b>nohangup</b> ] }	Optional. By default, the connection is disabled after executing the command automatically, and the delay time for executing the command automatically is 0.
Configure user livetime	<b>password-control livetime</b> <i>user-live-time</i>	Optional. By default, user livetime is not restricted.
Configure the maximum number of consecutive login authentication failures for administrator users	<b>password-control max-try-time</b> <i>max-try-time-number</i>	Optional. By default, user management does not set limits on the maximum number of attempts.
Configure the maximum number	<b>max-online-num</b> <i>user-number</i>	Optional.

Step	Command	Description
of online sessions for the same user.		By default, there is no limit to the maximum number of online sessions for the same user.
Configure the file permissions available to the user.	<b>fileSYS-control{read   write   execute   none}</b>	Optional. By default, the user has permissions to read, write, and execute.
Configure the directories provided by the device that can be accessed or managed by the administrator	<b>work-directory</b> <i>directory</i>	Optional. The default, it is the /flash directory. This attribute currently only serves to configure the file directory of the ftp user login device.
Configure user status	<b>stat { active / block }</b>	Optional. By default, the user status is active.

#### 14.2.4 Configure access user attributes

An access user is a user who accesses the network through a device.

##### Configuration Condition

None

##### Configure access user

Table 14-7 Configuring Access Users

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	
Create access user and enter access user mode at the same time.	<b>local-user</b> <i>user-name</i> class network	Mandatory. By default, no access user is configured.
Configure access user password	<b>password 0</b> <i>password</i>	Mandatory. By default, users do not have a password, which may prevent them from logging in to the device.
Set the type of server that access users can use.	<b>service-type { xauth }</b>	Mandatory. By default, a user does not support any service-type.
Set the user group to which the access user belongs.	<b>group</b> <i>group-name</i>	Optional. By default, the user group to which the access user belongs is not configured.
Configure user status	<b>stat { active / block }</b>	Optional. By default, the user status is active.

### 14.2.5 Configure local user groups

Local users are divided into the administrator user group and the access user group.

The administrator user group is a collection of administrator user attributes that support the configuration of password lifetime and the maximum number of consecutive login authentication failures.

The access user group manages access users, with hierarchical nesting, which more graphically reflects the organizational structure of the company or department relationship. No access user attributes are supported under the access user group at this time.

## Configuration Condition

None

### Configure administrator user group

Table 14-8 Configuring the Administrator User Group

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Create the administrator user group and enter the administrator user group mode	<b>manager-group</b> <i>group-name</i>	Mandatory. By default, no administrator user group is configured.
Configure the user password lifetime under the administrator user group	<b>password-control lifetime</b> <i>user-live-time</i>	Optional. By default, there is no limits set on the lifetime of administrator users under this user group, i.e., the password lifetime is subject to the one configured in the administrator user view.
Configure the maximum number of consecutive login authentication failures for users under the administrator user group.	<b>password-control max-try-time</b> <i>max-try-time-number</i>	Optional. By default, there is no limit to the number of consecutive login authentication failures for users under the administrator user group, that is, the maximum number of consecutive login authentication failures is subject to the one configured under the administrator user view.

## Configure Access User Groups

Table 14-9 Configuring Access User Groups

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	
Create the access user group and enter the access user group mode.	<b>user-group</b> <i>group-name</i>	Mandatory. By default, no access user group is configured.
Configure the parent group of the access user group.	<b>parent</b> <i>group-name</i>	Optional. By default, the parent group is seen as the parent path in the group name path.

### 14.2.6 Configure password policies

Our system has a strong password security policy. Password security is guaranteed from three aspects: password complexity, mandatory password change on first login, and a maximum number of password attempts. The password security policy is only valid for local administrator users.

#### Password Complexity:

- (1) Password has a minimum length requirement, and the administrator can set limits to the minimum length of the administrator user password. When setting a user password, if the length of the entered password is less than the minimum length set, the system will not allow the password to be set, and prompts "Bad password: It must contain at least 2 character(s)."
- (2) Password combination detection function where the administrator can set the type of combination of the elements that make up the user's password. The constituent elements of a password include the following four types:
  - Uppercase letters: [A to Z]

- Lowercase letters: [a~z]
- Decimal numbers: [0 to 9]
- 31 special characters (~! @\$%^&\*()\_+={}| \:;'"<>,. /')

There are 4 kinds of combinations of cryptographic elements, the specific meaning of each is as follows:

- Combination type 1 indicates that the password contains at least 1 element.
- Combination type 2 indicates that the password contains at least 2 elements.
- Combination type 3 indicates that the password contains at least 3 elements.
- Combination type 4 indicates that the password must contains all 4 elements.

When the user sets a password, the system checks whether the set password meets the configuration requirements, and only the password that meets the requirements can be set successfully.

(3) The password cannot be the same as the user name. When setting the administrator user password, if the password entered is the same as the user name, the system will not allow the password to be created.

#### **Mandatory Password Change at First Login:**

When the function of "User must change password when logging in for the first time" is enabled, the system will prompt the corresponding message upon the first login and ask the user to change the password, otherwise the user is not allowed to log in to the device. When the administrator user name is "admin", the user will be asked to change the password upon the first login, regardless of whether the "Mandatory password change on first login" function is enabled or not.

#### **Password lifetime:**

The password lifetime is used to limit the length of time a user's password can be used. When the password has been in use for longer than the password lifetime, the user is required to change the password. When a user logs in, if the user enters a password that has expired, the system will prompt that the password has expired and it must be reset before the local login can continue. If the password entered does not meet the requirements, or if the new password entered twice in a row does not match, the system will reject this login. For login in non-interactive mode, such as FTP user, after the password expires, the password of FTP user can only be changed by the administrator; however, if the password happens to expire during the login time period, it will not affect the login, however, the next FTP command will trigger offline. In particular, if the first login asks for a password change and the password has in fact reached its expiration time, the user will only be asked to change password once upon login.

#### **Maximum Number of Password Attempts:**

Setting limit on the maximum number of user attempts can be used to prevent malicious parties from decrypting passwords through multiple attempts. After the failed password attempt exceeds the maximum number of attempts, the system will add the user to the blacklist of the login-secure module, and the user account will be locked for a period of time.

## Configuration Condition

None

## Configuration Condition

Table 14-10 Configuring the Password Policy

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure password complexity	<b>password-control complexity</b> <b>{min-length <i>len</i>   with user-name-check   composition type-number <i>type-number</i> }</b>	Optional. By default, the minimum length of user password is 6, and there are 2 types of password element combination. User name and password are not allowed to be the same.
Configure users to mandatory password change on first login	<b>password-control firstmodify enable</b>	Optional. By default, users are not required to change their passwords for the first login.  Users with the administrator username "admin" will be required to change their password when they log in for the first time even if the command is not enabled.
Configure user livetime	<b>password-control livetime</b> <i>user-live-time</i>	Optional. By default, no limit is set on user lifetime.

Step	Command	Description
Configure the maximum number of consecutive login authentication failures for administrator users	<b>password-control max-try-time</b> <i>max-try-time-number</i>	Optional.  This command is configured in the administrator user group view and the administrator user view.  By default, the maximum number of consecutive login authentication failures for users under the administrator user group is not configured, i.e., the maximum number of consecutive login authentication failures is subject to the one configured under the administrator user view.

## 14.2.7 LUM Monitoring and Maintaining

Table 14-11 LUM Monitoring and Maintaining

Command	Description
<b>debug user { manager   network }</b>	Enable debug information for user management.
<b>show users class { manager   network } [ username ]</b>	Display user configuration information.
<b>show role [ rolename ]</b>	Display configuration information for all or specified roles.

## 14.3 Typical LUM Configuration Example

### 14.3.1 Configure network administrator users

#### Network Requirements

- Configure the network administrator user and verify user's network administrator privileges.

#### Network Topology

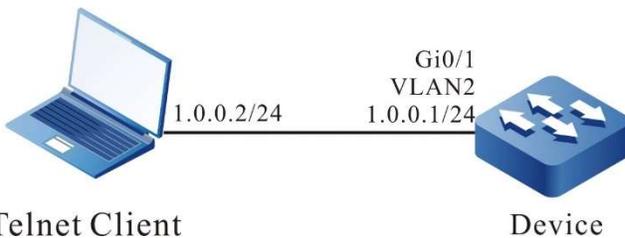


Figure 14-1 Network Topology for Configuring the Network Administrator User Group

#### Configuration Steps

Step 1: Configures IP addresses for the ports. (Omitted)

Step 2: Configure administrator attributes.

#Configure user admin, the password is admin.

```
Device#configure terminal
Device(config)#local-user admin class manager
Device(config-user-manager-admin)#password 0 admin
```

#Configuration service type

```
Device(config-user-manager-admin)#service-type telnet ftp web console ssh
```

#Configure the user role to which the local user belongs as network administrator.

```
Device(config-user-manager-admin)#user-role network-admin
```

#Configure local authorization to make the role effective

```
Device(config-user-manager-admin)#exit
Device(config)#domain system
Device(config-isp-system)#aaa authentication login local
Device(config-isp-system)#aaa authorization login local
Device(config-isp-system)#exit
```

#Configure login aaa authentication for line vty

```
Device(config)#line vty 0 15
Device(config-line)#login aaa
```

Step 3: Enters the username admin and password admin in the Telnet client to successfully log in to the device.

#Verify that the admin user can execute the admin command show logging to view the logs

```
Device#show logging
Logging source configurations
console is enabled,level: 7(debugging)
monitor is enabled,level: 7(debugging)
buffer is enabled,level: 5(notifications)
file is enabled,level: 7(debugging)
The Context of logging file:
```

#Verify that the network administrator cannot execute other administrator commands

```
Device#show role
You may not be authorized to perform this operation,please check.
```

---

### Note

- The default roles for administrators are security-admin, network-operator, audit-admin, and network-admin. You can set your administrator role as needed, or you can use custom roles.
- 

# 15 ZTP

---

## 15.1 Overview

ZTP (Zero Touch Provisioning) is a feature that automatically loads version files (including system software, configuration files, license files, patch files, custom files) when a newly shipped or unconfigured device is powered on.

It is designed to solve the problem that when deploying network device, after the hardware installation of the device is completed, the administrator needs to go to the installation site to debug the software of the device. When the devices are large in number and widely distributed, administrators manually

configuring each device affects the efficiency of deployment and labor costs in a bad way. The device runs ZTP function, which can get the version file from the USB disk or the file server and load it automatically to realize the field-free configuration and deployment of the device, thus reducing the labor cost and improving the deployment efficiency.

ZTP is not a standard protocol, it is a device zero-configuration deployment solution proposed by various vendors according to market demand, and there are differences in the details of implementation, but the basic process is the same. ZTP can be deployed in a number of ways, and we currently supports DHCP zero-configuration deployment, USB zero-configuration deployment and mail deployment. The process is to automatically enter the ZTP process by booting the device with empty configuration, first try to complete the automatic deployment through the inserted USB disk, and then try to complete the automatic deployment through DHCP if the USB disk deployment fails.

Network topology of a typical DHCP zero-configuration deployment is shown in Figure 15-1. When an empty-configuration device enters the DHCP zero-configuration deployment process, it will first broadcast DHCP discovery packets through the DHCP client. If the DHCP server is not in the same network segment with the zero-configuration device ready for employment, you need to configure a DHCP relay to send DHCP discovery packets across the network segments. When the DHCP server receives the DHCP discovery packets, it will assign temporary IP address, default gateway and other information for it, and return the intermediate file server address at the same time. The DHCP client receives the answering packet from the DHCP server, parses out the intermediate file server address and other information, downloads the intermediate file via FTP/TFTP/SFTP. In the end, it will parse the intermediate file, and download the corresponding version and configuration files from the intermediate file server according to the SN of this device (Serial Number device serial number). Reboot the device to take effect.

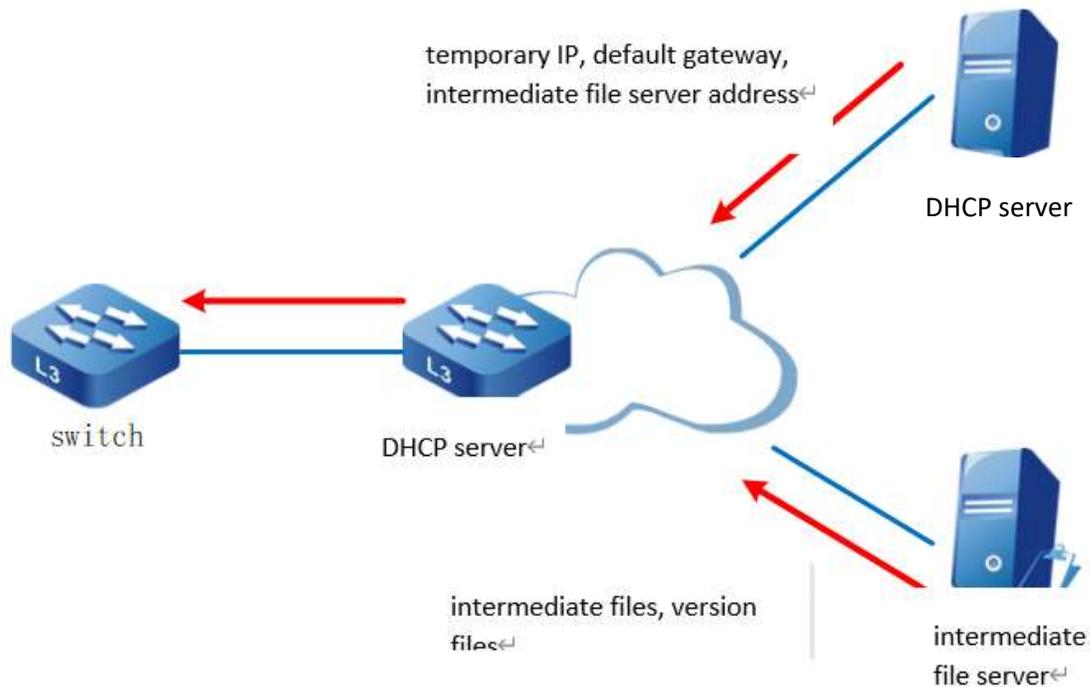


Figure 15-1 Typical Network Topology for DHCP

**DHCP server:** Used to assign temporary management IP address, default gateway, intermediate file server address and other information for the device executing ZTP.

**DHCP relay:** When the device executing ZTP and the DHCP server are in different network segments, it needs to forward the DHCP interaction packets through the DHCP relay.

**Intermediate file server:** Used to store intermediate files (intermediate file type is XML format), version files, configuration files, etc. needed by the device during the ZTP process. By parsing the intermediate file, the device executing ZTP can obtain information such as the file server address, the version file corresponding to this device, and the configuration file storage path. The intermediate file server supports TFTP, FTP, and SFTP types.

**Version file server:** Used to store the version files needed by the device, such as system software and configuration files. The version file server can be deployed on the same file server as the intermediate file server. It supports TFTP, FTP, and SFTP types.

In USB zero-configuration deployment process, the user edits the intermediate file, system version and configuration file and other information in advance and saves them in the USB. Then the USB is inserted into the device ready for zero-configuration deployment. When the device is powered on and detects the inserted USB with the intermediate file that meets the deployment requirements, it will enter the USB zero-configuration deployment process, compile the intermediate file according to the device SN, copy the corresponding system version and configuration files from the USB, and then reboot the device to take effect.

## 15.2 ZTP Function Configuration

### 15.2.1 Enable or Disable ZTP Function

Table 15-1 Enabling or Disabling the ZTP Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable the ZTP function	<b>ztp enable</b>	By default, ZTP function is enabled on the device.
Disable the ZTP function.	<b>no ztp enable</b>	-

---

## Note

- When ZTP is enabled or disabled, configuration is not displayed with the show running-config command. However, the configuration will take effect after rebooting.
- 

## 15.2.2 ZTP Monitoring and Maintaining

Table 15-2 ZTP Monitoring and Maintaining

Command	Description
<b>show ztp</b>	Display ZTP information
<b>[no] debug ztp</b>	Enable or disable ZTP debugging

## 15.3 ZTP Typical Configuration Example

### 15.3.1 Configure ZTP to use common intermediate files for zero-configuration deployment via DHCP

#### Network Requirements

- A PC is used as the Console control end to monitor the device ZTP start-up process.
- Device2 acts as the DHCP server and provides DHCP service for ZTP boot process.
- Server1 acts as the file server and provides the FTP service (or TFTP, SFTP service) needed for the ZTP startup process.
- Server2 acts as the log server and receives log information generated by the ZTP startup process.

#### Network Topology

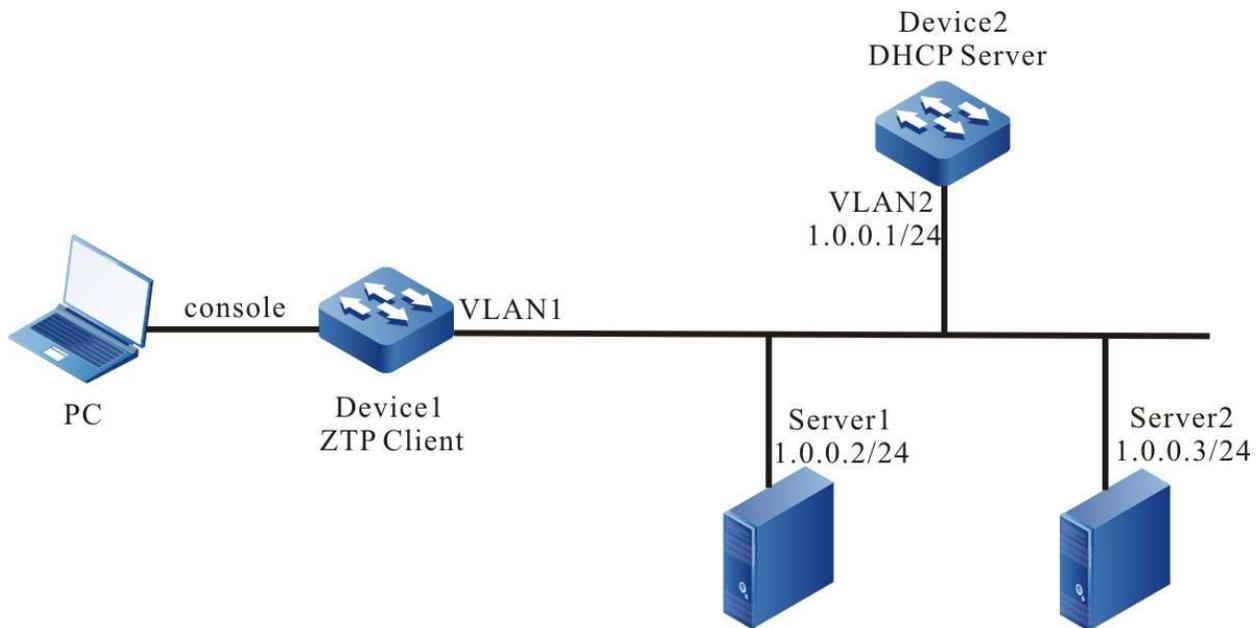


Figure 15-2 Network Topology of Device Using Common Intermediate Files for Zero-configuration Deployment via DHCP

### Configuration Steps

Step 1: Configure the FTP server and place the intermediate files (e.g. ztp.xml), version files and device configuration files downloaded into the the FTP server directory. (Omitted)

#Edit the common intermediate file as follows:

Right mouse click to open it in Excel and edit

Opening and Editing XML File in Excel

Determined as XML table and click OK.

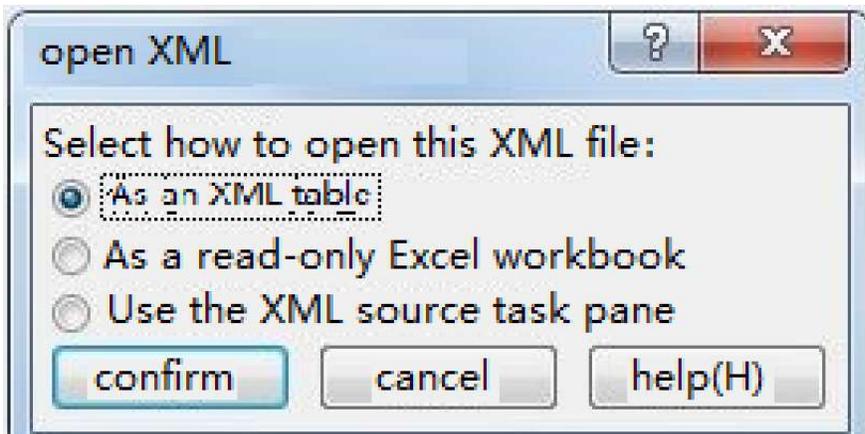


Figure 15-3 Determined as XML Table

Edit in Excel, here fill in the device serial number, version file name, version file name MD5 checksum value, configuration file name, configuration file MD5 checksum and description information, and finally save it, note that the it is saved in XML format.

	A	B	C	D
1	Serial-Number	Image-File	Image-File-MD5	Config-File
2	example_1:123456789	xxx.pck	xxx	startup
3	example_1:123456789			startup

Figure 15-4 Editing the Name of the Version and Configuration Files in the XML File

Step 2: Configure DHCP service for Device2.

```
Device2#configure terminal
Device2(config)#ip dhcp pool ztp
Device2(dhcp-config)#range 1.0.0.4 1.0.0.10 255.255.255.0
```

#Configure intermediate file name options

```
Device2(dhcp-config)#option 67 ascii ztp.xml
```

#Configuration file download method and server address, username and password options

```
Device2(dhcp-config)#option 66 ascii ftp://a:a@1.0.0.2
```

#Configure log server address options

```
Device2(dhcp-config)#option 7 ip 1.0.0.3
Device2(dhcp-config)#exit
```

#Enable DHCP service on server

```
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ip address 1.0.0.1/24
Device2(config-if-vlan2)#ip dhcp server
Device2(config-if-vlan2)#end
```

Step 3: Device1 boots with an empty configuration and enters the ZTP process to download the version upgrade and load the configuration file.

#See that the device enters the ZTP process through logs and sends DHCP requests

```
Apr 22 2020 06:03:58 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:123456789, Now starting dhcp upgrade...
Apr 22 2020 06:03:58 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:123456789, DHCP discovery phase started...
```

#During the ZTP request, you can exit the ZTP process with ctrl+c, thus starting with an empty configuration, or if you don't use ctrl+c, you can continue with the ZTP process.

```
Apr 22 2020 06:04:00 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:123456789, Press (ctrl + c) to abort Dhcp Upgrade
```

#Get the address successfully, download the common intermediate files

```
Apr 22 2020 06:04:35 Device1 MPU0 %DHCP-ASSIGNED_EXT-5:Interface vlan1 assigned DHCP address 1.0.0.4, mask 255.255.255.0.
Apr 22 2020 06:04:35 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:123456789, Dhcp discovery phase success
Apr 22 2020 06:04:35 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:123456789, Start to download temp file ztp.xml...
```

#Parse intermediate files and download version information

```
Apr 22 2020 06:04:35 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:123456789,Download temp file ztp.xml is success
Apr 22 2020 06:04:35 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:123456789,Start to parse temp file...
Apr 22 2020 06:04:35 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:123456789,parse temp file is success
Apr 22 2020 06:04:35 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:123456789,Start to download the Image file ztp.pck
```

#Download version and configuration file successfully, reboot the device automatically via ZTP

```
Apr 22 2020 06:09:26 Device1 MPU0 %SYS_UPDATE-RESULT-5:image : Mpu 0 upgrade successfully!
Apr 22 2020 06:12:26 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:123456789,Download the Image file is success
Apr 22 2020 06:12:26 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:123456789,Start to download the config file startup_ztp...
Apr 22 2020 06:12:26 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:123456789,Download the config file is success
Apr 22 2020 06:12:26 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:123456789,Dhcp upgrade is success
Apr 22 2020 06:12:26 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:123456789,System will rebooted by DHCP upgrade
```

Step 4: Check the result.

Check the ZTP status with the show ztp command, and view whether the configuration and version are in with show running-config and show version.

```
Device1#show ztp

Last ztp method: DHCP upgrade method
Ztp state: ZTP DHCP upgrade success
Ztp important information:
  FTP server IP: 1.0.0.2
  Temporary file name: ztp.xml
  Startup file name:startup_ztp
  Image file name:ztp.pck

Current ztp method: None upgrade method
```

---

## Note

- The device obtains the file download mode through option66 of DHCP protocol. It supports FTP, TFTP and SFTP, you can choose any download mode when during configuration.
  - If the version information of common intermediate file is empty, then the device ZTP process will not engage in version upgrade, only configuration loading to continue the ZTP process, however, the configuration file can not be empty.
-

- MD5 of version file and MD5 of configuration file are used for integrity check of version file and configuration file.
- In the case that no option66 option is issued, you can issue the TFTP server address directly through option 150. In such case, you can download intermediate files, version files, configuration files through the TFTP server.

### 15.3.2 Configure ZTP to use python intermediate files for zero-configuration deployment via DHCP

#### Network Requirements

- A PC is used as the Console control end to monitor the device ZTP start-up process.
- Device2 acts as the DHCP server and provides DHCP service for ZTP boot process.
- Server1 acts as the file server and provides the TFTP service (or FTP, SFTP service) needed for the ZTP startup process.
- Server2 acts as the log server and receives log information generated by the ZTP startup process.

#### Network Topology

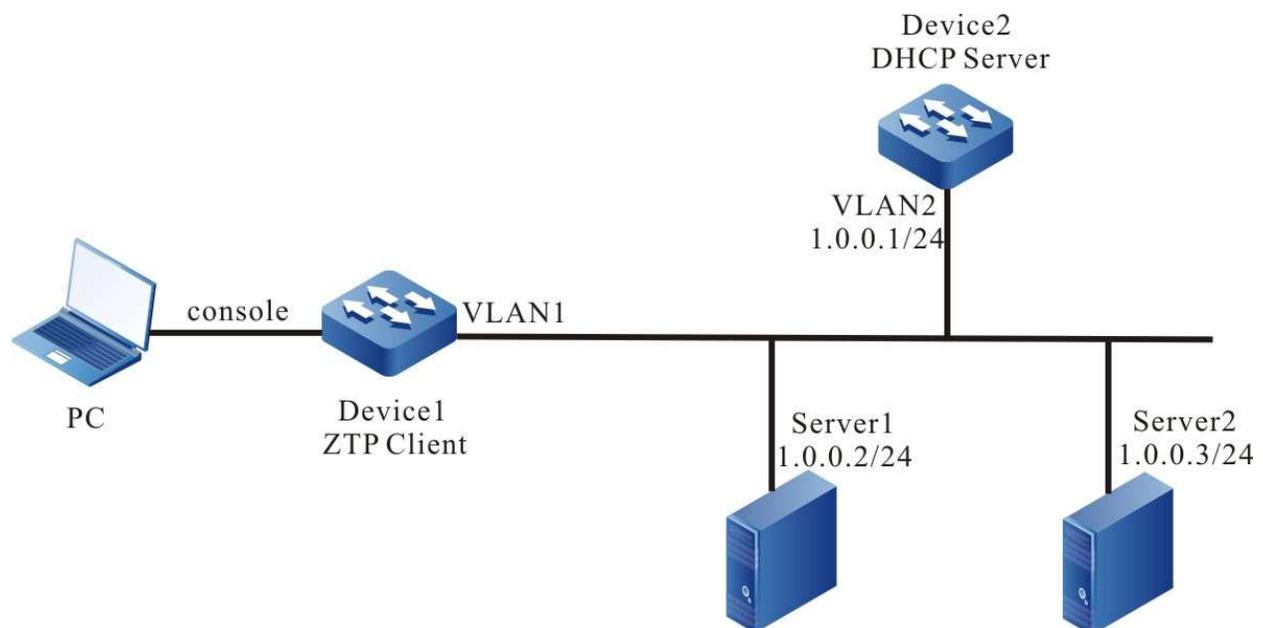


Figure 15-5 Network Topology of Device Using Python Intermediate Files for Zero-configuration Deployment via DHCP

#### Configuration Steps

Step 1: Configure the FTP server and place the intermediate files (e.g. ztp.py), version files and device configuration downloaded into the the FTP server directory. (Omitted)

#Normal python file editing can use any code editor

#Total file space required to configure ZTP

```
required_space = 100
```

#Configure file download method, and download timeout time

```
protocol = "tftp"  
username = ""  
password = ""  
hostname = "1.0.0.2"  
timeout = 1200
```

#Versions are found by version series, and version series can be found by shipping list

```
REMOTE_IMAGE_FILE = {  
    'HIT SW' : 'ztp.pck'  
}
```

#Configure remote paths to make it easy to find them on the server when downloading files over TFTP

```
remote_config_path = "/flash"  
remote_pck_path = ""
```

#Configure checksum MD5

```
remote_config_is_exist_md5 = False  
remote_pck_is_exist_md5 = False
```

Step 2: Configure DHCP service for Device2.

```
Device2#configure terminal  
Device2(config)# ip dhcp pool ztp  
Device2(dhcp-config)#range 1.0.0.4 1.0.0.10 255.255.255.0
```

#Configure intermediate file name options

```
Device2(dhcp-config)#option 67 ascii ztp.py
```

#Configuration file download method and server address, username and password options

```
Device2(dhcp-config)#option 66 ascii tftp://1.0.0.2
```

#Configure log server address options

```
Device2(dhcp-config)#option 7 ip 1.0.0.3  
Device2(dhcp-config)#exit
```

#Enable DHCP service on server

```
Device2(config)#interface vlan2  
Device2(config-if-vlan2)#ip address 1.0.0.1/24  
Device2(config-if-vlan2)#ip dhcp server  
Device2(config-if-vlan2)#end
```

**Step 3:** Device1 boots with an empty configuration and enters the ZTP process to download the version upgrade and load the configuration file.

**#See that the device enters the ZTP process through logs and sends DHCP requests**

```
Apr 22 2020 06:03:58 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:123456789, Now starting dhcp upgrade...
Apr 22 2020 06:03:58 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:123456789, DHCP discovery phase started...
```

**#During the ZTP request, you can exit the ZTP process with ctrl+c, thus starting with an empty configuration, or if you don't use ctrl+c, you can continue with the ZTP process.**

```
Apr 22 2020 06:04:00 Device1MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:123456789, Press (ctrl + c) to abort Dhcp Upgrade
```

**#Get the address successfully, download the common intermediate files**

```
Apr 22 2020 06:04:35 Device1 MPU0 %DHCP-ASSIGNED_EXT-5:Interface vlan1 assigned DHCP address 1.0.0.4, mask 255.255.255.0.
Apr 22 2020 06:04:35 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:123456789, Dhcp discovery phase success
Apr 22 2020 06:04:35 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:123456789, Start to download temp file ztp.py...
Apr 22 2020 06:04:35 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:123456789, Download temp file ztp.py is success
Apr 22 2020 06:04:35 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:123456789, Start to parse temp file...
```

**#Direct execution of python scripts**

```
Execute python script start ...
/flash free space is 168(M).
Start to get remote and local file path.
remote config path is /flash/123456789.cfg
Get remote and local file path is success.
remote PCK path is ztp.pck
Start to download image file ztp.pck...
Download image file is success
Start to set boot image file /flash/ztp.pck...
```

**#Download version and configuration file successfully, reboot the device automatically via ZTP**

```
Apr 22 2020 06:09:26 Device1 MPU0 %SYS_UPDATE-RESULT-5:image : Mpu 0 upgrade successfully!
Set boot image file is success.
Start to download config file /flash/123456789.cfg...
Download config file is success.
Start to parse config file /flash/startup...
Parse config file is success.
Execute python script success.
```

```
Apr 22 2020 06:12:26 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:123456789,script execute success
Apr 22 2020 06:12:26 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:123456789,System will rebooted by DHCP upgrade
```

**Step 4:** Check the result.

Check the ZTP status with the show ztp command, and view whether the configuration and version are in with show running-config and show version.

```
Device1#show ztp
```

```
Last ztp method: DHCP upgrade method
Ztp state: ZTP DHCP upgrade success
Ztp important inforamtion:
  TFTP server IP: 1.0.0.2
  Temporary file name: ztp.py
```

```
Current ztp method: None upgrade method
```

---

## Note

- The device obtains the file download mode through option66 of DHCP protocol. It supports FTP, TFTP and SFTP, you can choose any download mode when during configuration.
  - The server download method issued by the DHCP server is used to download intermediate files, and the download method set in the python file is used to download version files and configuration files, which are not necessarily related.
  - If the version information is not found through the device serial number, then the device ZTP process will not engage in version upgrade, only configuration loading to continue the ZTP process, however, the configuration file cannot be empty.
  - If the file download method is TFTP, the username and password fields must be empty strings, and you cannot directly delete those two parameters.
  - The name of the configuration file downloaded by the device is based on the serial number with the suffix .md5. For example, the device serial number is 12345, then the configuration file name is 12345.md5, and the MD5 checksum file is 12345.cfg.md5.
  - After downloading the python file, the device executes the python file directly, so the python file must conform to the python syntax.
- 

### 15.3.3 Configure ZTP to use common intermediate files for zero-configuration deployment via

#### USB

##### Network Requirements

- A PC is used as the Console control end to monitor the device ZTP start-up process.
- Device1 is inserted with an USB device, which contains intermediate files, version files, and device configuration files.

##### Network Topology

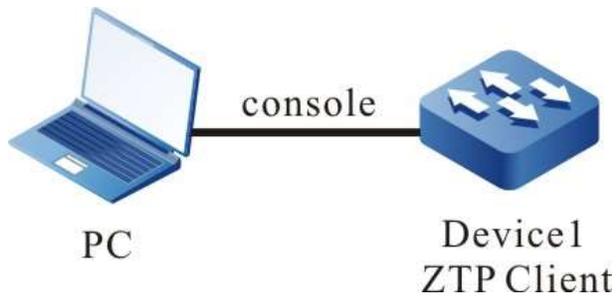


Figure 15-6 Network Topology of Device Using Common Intermediate Files for Zero-configuration Deployment via USB

### Configuration Steps

Step 1: Place the intermediate file in the USB root directory and name it `ztp_config.xml`, i.e. `/usb/ztp_config.xml`.

#Edit the common intermediate file as follows:

Right mouse click to open it in Excel and edit

Opening and Editing XML File in Excel

Determined as XML table and click OK.

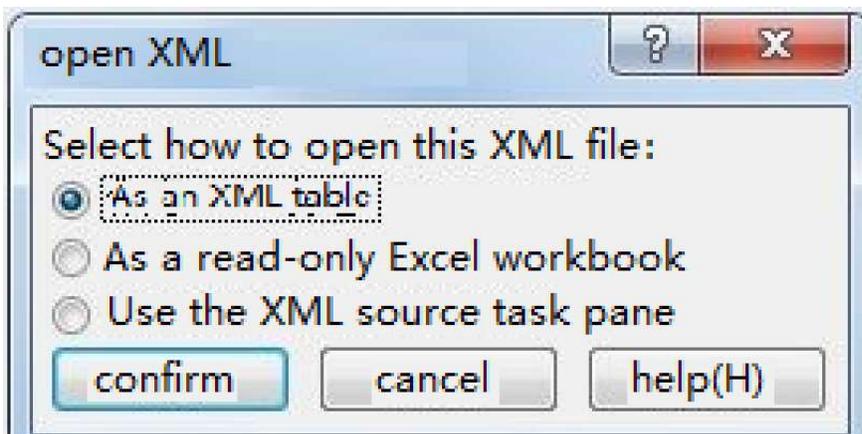


Figure 15-7 Determined as XML Table

Edit in Excel, here fill in the device serial number, version file name, version file name MD5 checksum value, configuration file name, configuration file MD5 checksum and description information, and finally save it, note that the it is saved in XML format.

	A	B	C	D
1	Serial-Number	Image-File	Image-File-MD5	Config-File
2	example_1:123456789	xxx.pck	xxx	startup
3	example_1:123456789			startup

Figure 15-8 Editing the Name of the Version and Configuration Files in the XML File

### Note

- XXX is the name of the corresponding IOS version in the USB.
- The XML intermediate file is obtained from the ZTP path of the software release notes.
- In the XML intermediate file, the required fields are serial number, version and configuration file. The serial number can be obtained from the device shipping list; the version file name and configuration file name filled in the xml intermediate file must be consistent with the IOS version file name and configuration file name in the USB, otherwise the deployment will fail.
- The version file MD5 code, configuration file MD5 code, and description information in the XML intermediate file are optional. If you need to fill in the MD5 code, it can be generated by a common MD5 code calculator.

**Step 2:** The version file and configuration file corresponding to the device serial number in the intermediate file are placed into the USB root directory, and named the same as described in the intermediate file. (Omitted)

**Step 3:** The device is powered on and enters the ztp process for deployment via USB.

#Device configuration is empty, enter USB deployment process

```
the current config file /flash/startup does not exist.
The backup file /backupramfs/startup is not exist.
The current config file /backup/startup does not exist.
May 6 2020 15:16:15 Device1 MPU0 %ZTP-USB_UPGRADE-5:SerialNum:123456789,Now starting USB upgrade...
```

#Find and parse intermediate files

```
May 6 2020 15:16:15 Device1 MPU0 %ZTP-USB_UPGRADE-5:SerialNum:123456789,Start to copy the temporary file /usb/ztp_config.xml...
May 6 2020 15:16:15 Device1 MPU0 %ZTP-USB_UPGRADE-5:SerialNum:123456789,Copy the temporary file is success.
May 6 2020 15:16:15 Device1 MPU0 %ZTP-USB_UPGRADE-5:SerialNum:123456789,Start to parse the temporary file /flash/ztp_config.xml
```

## #Upgraded versions and configurations

```
May 6 2020 15:16:15 Device1 MPU0 %ZTP-USB_UPGRADE-5:SerialNum:123456789,Parse temporary file is success
May 6 2020 15:19:53 Device1 MPU0 %ZTP-USB_UPGRADE-5:SerialNum:123456789,Sysupdate image is success
May 6 2020 15:19:53 Device1 MPU0 %ZTP-USB_UPGRADE-5:SerialNum:123456789,Start to copy config...
May 6 2020 15:19:54 Device1 MPU0 %ZTP-USB_UPGRADE-5:SerialNum:123456789,Copy config is success
```

## #Reboot after upgrade

```
May 6 2020 15:19:54 Device1 MPU0 %ZTP-USB_UPGRADE-4:SerialNum:123456789,System will be rebooted by USB Upgrade
```

Step 4: Check the results.

#Check the ZTP status with the show ztp command, and view whether the configuration and version are in with show running-config and show version.

```
Device1#show ztp
```

```
Last ztp method: USB upgrade method
Ztp state: ZTP USB Upgrade success
Ztp important information:
  Temporary file name:/usb/ztp_config.xml
  Startup file name:startup
  Image file name:ztp.pck
```

```
Current ztp method: None upgrade method
```

```
Next ztp state: disable
```

---

### Note

- If the version information of common intermediate file is empty, then the device ZTP process will not engage in version upgrade, only configuration loading to continue the ZTP process, however, the configuration file can not be empty.
  - The device will download the version and configuration file from the USB copy, so the version file and the configuration file need to be placed into the USB.
  - The name of the common intermediate file in USB can only be ztp\_config.xml.
- 

## 15.3.4 Configure ZTP to use python intermediate files for zero-configuration deployment via USB

### Network Requirements

- A PC is used as the Console control end to monitor the device ZTP start-up process.
- Device1 is inserted with an USB device, which contains intermediate files, version files, and device configuration files.

### Network Topology

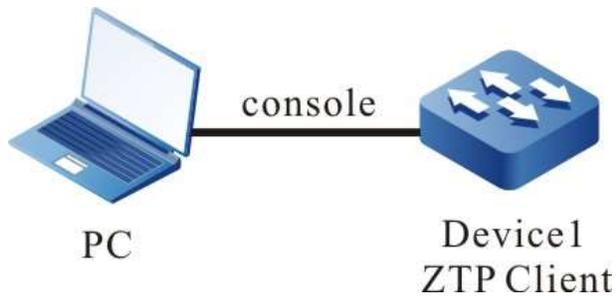


Figure 15-9 Network Topology of Device Using Python Intermediate Files for Zero-configuration Deployment via USB

### Configuration Steps

Step 1: Place the intermediate file in the USB root directory and name it `ztp_script.py`, i.e. `/usb/ztp_script.py`.

#Normal python file editing can use any code editor

#Total file space required to configure ZTP (Unit: MB)

```
required_space = 100
```

#Versions are found by version series, and version series can be found by shipping list

```
REMOTE_IMAGE_FILE = {
'HIT SW': 'ztp.pck'
}
```

#Configure the remote path and look for version files and configuration files in the `/usb` path

```
remote_config_path = "/usb"
remote_pck_path = "/usb"
```

Step 2: Copy the version file and the device configuration file to the USB root directory. The version name must be the same as the version file name corresponding to the device serial number in the intermediate file, and the configuration file name is consisting of the device serial number plus the `.cfg` suffix. For example, if the device serial number is 12345, then the configuration file name is `12345.cfg`. (Omitted)

Step 3: The device is inserted with the USB and enters the `ztp` process for deployment via USB when powered on.

#Configuration file does not exist, the USB is plugged into the device, the device enters ZTP deployment process via USB.

The current config file `/flash/startup` does not exist.

The backup file /backupramfs/startup is not exist.  
The current config file /backup/startup does not exist.  
Apr 30 2020 11:10:12 Device1 MPU0 %SYS\_UPDATE-RESULT-5:SerialNum:123456789,Now starting USB upgrade...

### #Find and parse intermediate files

Apr 30 2020 11:10:12 Device1 MPU0 %SYS\_UPDATE-RESULT-5:SerialNum:123456789,Start to copy the temporary file /usb/ztp\_script.py...  
Apr 30 2020 11:10:12 Device1 MPU0 %SYS\_UPDATE-RESULT-5:SerialNum:123456789,Copy the temporary file is success.  
Apr 30 2020 11:10:12 Device1 MPU0 %SYS\_UPDATE-RESULT-5:SerialNum:123456789,:Start to parse the temporary file /flash/ztp\_script.py

### #Invoke python to execute intermediate files

Execute python script start ...

### #Check the remaining space

/flash free space is 159(M).

### #Download configuration and version files

Start to get remote and local file path.  
Get remote and local file path is success.  
Start to set boot image file /usb/ztp.pck...  
Apr 30 2020 11:13:51 Device1 MPU0 %SYS\_UPDATE-RESULT-5:SerialNum:123456789,image : Mpu 0 upgrade successfully!Set boot image file is success.  
Start to copy config file /usb/12345.cfg...  
Copy config file is success.  
Start to parse config file /flash/startup...  
Parse config file is success.

### #Download successfully, restart for the version and configuration to take effect.

Execute python script success, reboot device.  
Apr 30 2020 11:13:54 Device1 MPU0 %SYS\_UPDATE-RESULT-5:SerialNum:123456789,script execute success  
Apr 30 2020 11:13:54 Device1 MPU0 %SYS\_UPDATE-RESULT-4:SerialNum:123456789,System will be rebooted by USB Upgrade

Step 4: Check the results.

#Check the ZTP status with the show ztp command, and view whether the configuration and version are in with show running-config and show version.

Device1#show ztp

Last ztp method: USB upgrade method  
Ztp state: ZTP USB Upgrade success  
Ztp important information:  
Temporary file name:/usb/ztp\_script.py  
Startup file name:startup  
Image file name:ztp.pck

Current ztp method: None upgrade method

Next ztp state: disable

---

## Note

- After downloading the python file, the device executes the python file directly, so the python file must conform to the python syntax.
  - The device obtains the file download mode through option66 of DHCP protocol.
-

---

It supports FTP, TFTP and SFTP, you can choose any download mode when during configuration.

- If the version information is not found through the device serial number, then the device ZTP process will not engage in version upgrade, only configuration loading to continue the ZTP process, however, the configuration file cannot be empty.
  - The name of the configuration file downloaded by the device is based on the serial number with the suffix .md5. For example, the device serial number is 12345, then the configuration file name is 12345.md5, and the MD5 checksum file is 12345.cfg.md5.
  - The device will download the version and configuration file from the USB copy, so the version file and the configuration file need to be placed into the USB.
  - The name of the common intermediate file in USB can only be ztp\_script.py.
- 

### 15.3.5 Configure ZTP to automatically complete stacking using python intermediate files via DHCP

#### Network Requirements

- PC1 is used as the Console control end to monitor the device ZTP start-up process.
- Device3 acts as the DHCP server and provides DHCP service for ZTP boot process.
- Server1 acts as the file server and provides the FTP service (or TFTP, SFTP service) needed for the ZTP startup process.
- Server2 acts as the log server and receives log information generated by the ZTP startup process.
- Device1 and Device2 complete stacking through Te0/50 as a stacking link.

#### Network Topology

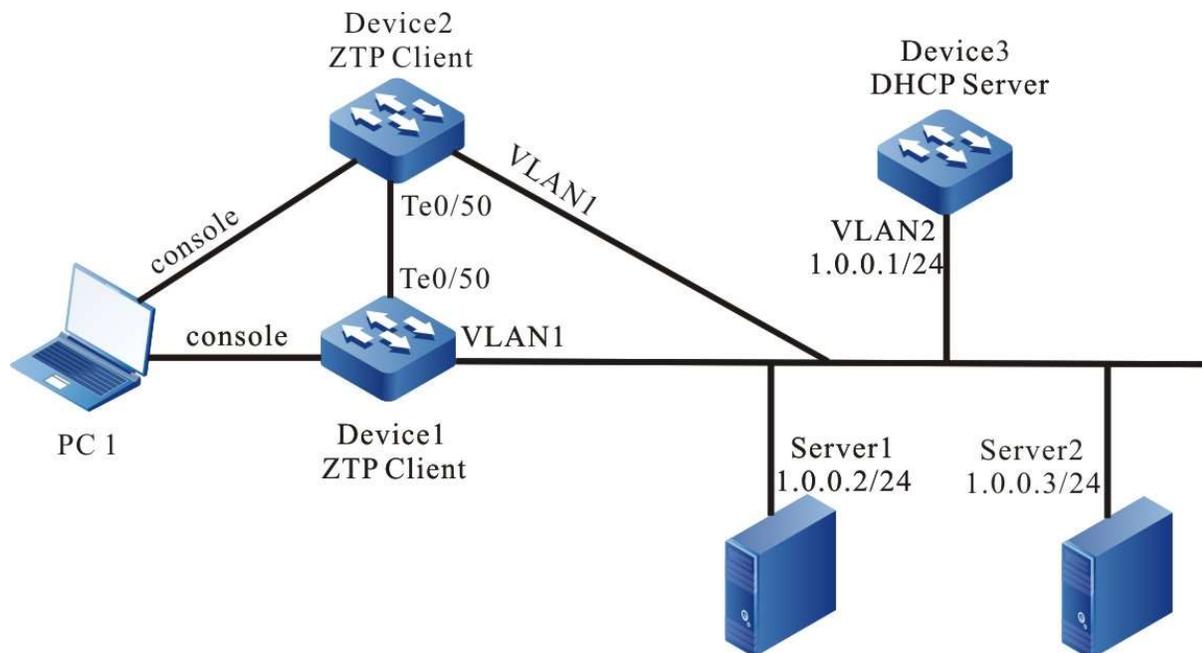


Figure 15-10 Network Topology of ZTP using python intermediate files to automatically complete stacking via DHCP

### Configuration Steps

Step 1: Configure the FTP server, edit the intermediate files, and place the intermediate files (e.g. ztp.py) and the version file corresponding to the serial number in the FTP server directory. (Omitted)

#Normal python file editing can use any code editor

#Total file space required to configure ZTP

```
required_space = 100
```

#Configure file download method, and download timeout time

```
protocol = "ftp"
username = "a"
password = "a"
hostname = "1.0.0.2"
timeout = 1200
```

#Versions are found by version series, and version series can be found by shipping list

```
REMOTE_IMAGE_FILE = {
'HIT SW' : 'ztp.pck'
}
```

#Configure remote paths to make it easy to find them on the server when downloading files over FTP

```
remote_config_path = ""
remote_pck_path = ""
```

```
remote_stack_path = ""
```

### #Configure checksum MD5

```
remote_config_is_exist_md5 = True
remote_pck_is_exist_md5 = True
remote_stack_is_exist_md5 = True
```

Step 2: Edit stack files and configuration files and upload them to the server for ZTP process download.

Here it is assumed that the device serial number of Device1 is 12345 and the device serial number of Device2 is 12340.

### #Edit stack files

Stack file is named by adding .stack to the serial number. The name of Device1 stack file is 12345.stack, and the corresponding MD5 checksum file is 12345.stack.md5, while the name of Device2 stack file is 12340.stack, and the corresponding MD5 checksum file is 12340.cfm.md5.

Stack file content: It contains serial number, stacking domain number, and stacking device member.

The content of Device1's stack file includes

```
12345 101 1
```

The content of Device2's stack file includes

```
12340 101 0
```

#Edit the configuration file, the configuration file is named by adding the suffix .cfg to the device serial number, so the name of Device1 configuration file is 12345.cfg, and the corresponding MD5 checksum file is 12345.cfg.md5, while the name of Device2 configuration file is 12340.cfg, and the corresponding MD5 checksum file is 12340.cfm.md5.

The stacking section of the configuration file must be included with !VST\_CONFIG\_BEGIN and !VST\_CONFIG\_END, the slot port configuration must be included with !PORT\_CONFIG\_BEGIN and !PORT\_CONFIG\_END, and the interface dimension set in the configuration file must be the stacked interface dimension, not the standalone dimension.

The configuration file of Device1 contains

```
!VST_CONFIG_BEGIN
!mode vsl information
vsl-channel 1/1
exit
!mode vsl end

!PORT_CONFIG_BEGIN
!slot 0/0
interface tengigabitethernet1/0/50
vsl-channel 1/1 mode on
exit
!PORT_CONFIG_END
!VST_CONFIG_END
```

The configuration file of Device2 contains

```
!VST_CONFIG_BEGIN
!mode vsl information
vsl-channel 0/1
exit
!mode vsl end

!PORT_CONFIG_BEGIN
!slot 0/0
interface tengigabitethernet0/0/50
vsl-channel 0/1 mode on
exit
!PORT_CONFIG_END
!VST_CONFIG_END
```

After uploading the configuration file and stack files to the server, the following files 12345.cfg, 12340.cfg, 12345.cfg.md5, 12340.cfg.md5 exist on the server.

### Step 3: Configure DHCP service for Device3.

```
Device3#configure terminal
Device3(config)# ip dhcp pool ztp
Device3(dhcp-config)#range 1.0.0.4 1.0.0.10 255.255.255.0
```

#### #Configure intermediate file name options

```
Device3(dhcp-config)#option 67 ascii ztp.py
```

#### #Configuration file download method and server address, username and password options

```
Device3(dhcp-config)#option 66 ascii ftp://a:a@1.0.0.2
```

#### #Configure log server address options

```
Device3(dhcp-config)#option 7 ip 1.0.0.3
Device3(dhcp-config)#exit
```

#### #Enable DHCP service on server

```
Device3(config)#interface vlan2
Device3(config-if-vlan2)#ip address 1.0.0.1/24
Device3(config-if-vlan2)#ip dhcp server
Device3(config-if-vlan2)#end
```

Step 4: Device1 and Device2 boot with an empty configuration and enters the ZTP process to download the version upgrade and load the configuration file.

Device1:

#### #See that the device enters the ZTP process through logs and sends DHCP requests

```
Apr 22 2020 06:03:58 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:12345, Now starting dhcp upgrade...
Apr 22 2020 06:03:58 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:12345, DHCP discovery phase started...
```

#During the ZTP request, you can exit the ZTP process with ctrl+c, thus starting with an empty configuration, or if you don't use ctrl+c, you can continue with the ZTP process.

```
Apr 22 2020 06:04:00 Device1MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:12345, Press (ctrl + c) to abort Dhcp Upgrade
```

## #Get the address successfully, download the common intermediate files

```
Apr 22 2020 06:04:35 Device1 MPU0 %DHCP-ASSIGNED_EXT-5:Interface vlan1 assigned DHCP address 1.0.0.4, mask 255.255.255.0.
Apr 22 2020 06:04:35 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:12345, Dhcp discovery phase success
Apr 22 2020 06:04:35 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:12345, Start to download temp file ztp.py...
Apr 22 2020 06:04:35 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:12345, Download temp file ztp.py is success
Apr 22 2020 06:04:35 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:12345, Start to parse temp file...
```

## #Direct execution of python scripts

```
/flash free space is 100(M).
Start to get remote and local file path.
Get remote and local file path is success.
```

## #Download version

```
Start to download image file /flash/ztp.pck...
Download image file is success
Start to set boot image file /flash/ztp.pck....
```

## #Download and parse stack file and configuration file

```
Start to download stack file /flash/12345.stack...
Download stack file is success.
Start to download config file /flash/12345.cfg...
Download config file is success.
Start to parse config file /flash/startup...
Parse config file is success.
Execute python script success.
```

## #Download version and configuration file successfully, reboot the device automatically via ZTP

```
Apr 22 2020 06:12:26 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:12345,script execute success
Apr 22 2020 06:12:26 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:12345,System will rebooted by DHCP upgrade
```

The device Device2:

## #See that the device enters the ZTP process through logs and sends DHCP requests

```
Apr 22 2020 06:03:58 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:12340, Now starting dhcp upgrade...
Apr 22 2020 06:03:58 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:12340, DHCP discovery phase started...
```

#During the ZTP request, you can exit the ZTP process with ctrl+c, thus starting with an empty configuration, or if you don't use ctrl+c, you can continue with the ZTP process.

```
Apr 22 2020 06:04:00 Device1MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:12340, Press (ctrl + c) to abort Dhcp Upgrade
```

## #Get the address successfully, download the common intermediate files

```
Apr 22 2020 06:04:35 Device1 MPU0 %DHCP-ASSIGNED_EXT-5:Interface vlan1 assigned DHCP address 1.0.0.5, mask 255.255.255.0.
Apr 22 2020 06:04:35 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:12340, Dhcp discovery phase success
Apr 22 2020 06:04:35 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:12340, Start to download temp file ztp.py...
Apr 22 2020 06:04:35 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:12340, Download temp file ztp.py is success
Apr 22 2020 06:04:35 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:12340, Start to parse temp file...
```

## #Direct execution of python scripts

```
/flash free space is 101(M).
Start to get remote and local file path.
Get remote and local file path is success.
```

## #Download version

```
Start to download image file /flash/ztp.pck...
Download image file is success
Start to set boot image file /flash/ztp.pck....
```

## #Download and parse stack file and configuration file

```
Start to download stack file /flash/12340.stack...
Download stack file is success.
Start to download config file /flash/12340.cfg...
Download config file is success.
Start to parse config file /flash/startup...
Parse config file is success.
Execute python script success.
```

## #Download version and configuration file successfully, reboot the device automatically via ZTP

```
Apr 22 2020 06:12:26 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:12340,script execute success
Apr 22 2020 06:12:26 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:12340,System will rebooted by DHCP upgrade
```

### Step 5: Check the result.

Check the ZTP status with the show ztp command, view whether the configuration and version are in with show running-config and show version, and view that the stack has taken effect with show vst-config.

```
switch#show ztp
```

```
Last ztp method: DHCP upgrade method
Ztp state: ZTP DHCP upgrade success
Ztp important inforamtion:
  FTP server IP: 1.0.0.2
  Temporary file name: ztp.py
```

```
Current ztp method: None upgrade method
```

```
Next ztp state: Next ztp state: disable(Stack mode does not support ztp.)
```

```
switch X#show vst-config
Building Configuration...
```

```
!mode member information
switch mode virtual
switch virtual member 0
  domain 101
  exit
switch virtual member 1
  domain 101
  exit
!mode member end
```

```
!mode vsl information
User manual
Release 1.0 01/2022
```

```
vsl-channel 0/1
exit
vsl-channel 1/1
exit
!mode vsl end
```

```
!slot_0_SM89E-48XGEF-DB(V1)
!vsl mode
!slot 0/0
interface tengigabitethernet0/0/50
vsl-channel 0/1 mode on
exit
!end
```

```
!slot_14_SM89E-48XGEF-DB(V1)
!vsl mode
!slot 1/0
interface tengigabitethernet1/0/50
vsl-channel 1/1 mode on
exit
!end
```

---

## Note

- The device obtains the file download mode through option66 of DHCP protocol. It supports FTP, TFTP and SFTP, you can choose any download mode when during configuration.
  - The MD5 of version files, configuration files, and stack files are stored separately, and they are named by adding the the suffix .md5. to their respective files names.
  - The interface dimension in the configuration file for auto-stacking must be the stacked interface dimension, not the standalone interface dimension.
  - After downloading the python file, the device executes the python file directly, so the python file must conform to the python syntax.
  - If the version information is not found through the device serial number, then the device ZTP process will not engage in version upgrade, only configuration loading to continue the ZTP process, however, the configuration file cannot be empty.
-

# 16 Interface Basis

---

## 16.1 Overview

The interfaces supported by the device include physical interfaces and logical interfaces. The physical interfaces include L2 Ethernet interfaces and L3 Ethernet interfaces; the logical interfaces include aggregation group interfaces, VLAN interfaces, Loopback interfaces, Null interfaces, Tunnel interfaces, and so on.

Ethernet interface, also called L2 Ethernet interface or port, is one physical interface. It works in layer 2 in the OSI reference model-Data link layer and is mainly used for the data frame forwarding and MAC address learning.

L3 Ethernet interface is one physical interface. It works at layer 3 in the OSI reference model-network layer. Configurable with an IP address, it is mainly used for packet forwarding.

Aggregation group interface is one logical interface, formed by binding multiple physical links between two devices. It also works at the data link layer and is mainly used to expand the link bandwidth and improve the link reliability.

VLAN interface is one logical interface, used to be bound with VLAN and complete the packet forwarding between different VLANs.

Loopback interface, also called local loopback interface, is one logical interface. For packets sent to the Loopback interface, the device considers each packet to be sent to itself and will not forward the packet.

Null interface is one logical interface. Any packet sent to the Null interface will be dropped.

Tunnel interface is one logical interface that provides a transmission link for the point-to-point mode.

For different interfaces, there are corresponding configuration modes. The related configuration modes of the interfaces include:

- interface configuration mode, corresponding to the VLAN interface, the Loopback interface, the Null interface, and the Tunnel interface;

- L2 Ethernet interface configuration mode, corresponding to the L2 Ethernet interface;
- L3 Ethernet interface configuration mode, corresponding to the L3 Ethernet interface;  
and
- aggregation group configuration mode, corresponding to the aggregation group interface.

This chapter mainly describes the common function configuration of various interfaces. For the featured function configuration of various interfaces, refer to the corresponding interface chapter.

## 16.2 Basic Function Configuration of Interfaces

Table 1 Basic Function Configuration List of Interfaces

Configuration Task	
Configure the basic functions of the interfaces	Enable/disable interface
	Configure interface description
	Configure the statistics interval of the interface traffic
Configure the interface group function	Interface groups
Configure interface status SNMP agent care level	Configure interface status SNMP agent care level

### 16.2.1 Configure the basic functions of the interfaces

#### Configuration Condition

None

#### Enable/disable interface

After Ethernet interface is disabled, it cannot receive or send packets. But after the Ethernet interface is enabled, whether it can receive and send packets also depends on other settings, such as whether the peer Ethernet interface is enabled, the rates of the local port and the peer port, and whether duplex mode matches with MDIX (Media Dependent Interface Crossover).

After the aggregation group interface is disabled, all member ports are disabled; after the aggregation group interface is enabled, you can disable or enable one member port separately.

Table 2 Enabling/Disabling Interface

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	At least one option must be selected.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	The subsequent configuration takes effect only on the current interface after you enter the interface configuration mode, only on the aggregation group
Enter the L2/L3 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	interface after you enter the aggregation group configuration mode, only on the current interface after you enter the L2/L3 Ethernet interface configuration mode, and only on the current virtual switch link interface after you enter the virtual switch link interface mode
Enter virtual switch link interface configuration mode	<b>vsl-channel</b> <i>vsl-channel-id</i>	
Enable the interface	<b>no shutdown</b>	Mandatory By default, the interface is enabled
Disable the interface	<b>shutdown</b>	Mandatory By default, the interface is enabled

---

### Note

- Configure the interface enabling/disabling function, which is not supported on Null interface.
- 

### Configure interface description

The interface description is used for naming different interfaces, helping the user distinguish different interface types and actual service functions. It is convenient for the user to manage various interfaces.

Table 16 Configuring Interface Description Information

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	At least one option must be selected.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	The subsequent configuration takes effect only on the current interface after you enter the interface configuration mode, only on the aggregation group
Enter the L2/L3 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	interface after you enter the aggregation group configuration mode, only on the current interface after you enter the L2/L3 Ethernet interface configuration mode, and only on the current virtual switch link interface after you enter the virtual switch link interface mode
Enter virtual switch link interface configuration mode	<b>vsl-channel</b> <i>vsl-channel-id</i>	
Configure interface description information	<b>description</b> <i>description-name</i>	Mandatory By default, the interface description information is not configured
	<b>peer-description</b> <i>description-name</i>	Mandatory By default, the peer interface description information is not configured

---

 **Note**

- Configure the interface description function, which is not supported on Null interface.
- 

### Configure the statistics interval of the interface traffic

Different interfaces carry different service traffics. Adjusting the statistics interval of the interface traffic can help the user concern the history records of the interface traffic selectively, forecasting the future trend of the interface traffic more correctly. It is convenient for the user to analyze and adjust the bored services of the interface.

Table 3 Configuring Statistics Interval of Interface Traffic

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	At least one option must be selected.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	The subsequent configuration takes effect only on the current interface after you enter the interface configuration mode, only on the aggregation group interface after you enter the aggregation group configuration mode, only on the current port after you enter the L2 Ethernet interface configuration mode, and only on the current virtual switch link interface after you enter the virtual switch link interface mode
Enter the L2/L3 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	
Enter virtual switch link interface mode	<b>vsl-channel</b> <i>vsl-channel-id</i>	
Configure the statistics interval of the interface traffic	<b>load-interval</b> <i>load-interval-value</i>	Mandatory

Step	Command	Description
		By default, the statistics interval of the interface traffic is 300 seconds.

## Note

- Configure the statistics interval function of interface traffic, which is not supported on Null interface.

### 16.2.2 Configure the interface group function

Bind multiple interfaces as one interface group. Configuring various interface commands on the interface group is equivalent to configuring on all interfaces of the interface group, while it is not necessary to configure on each interface repeatedly. Display the information of one interface group is to display the information of all interfaces in the interface group.

#### Configuration Condition

The interfaces covered by the interface group should already exist.

#### Interface groups

Table 4 Configuring Interface Group

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Create interface group in the list mode	<b>interface group</b> <i>group-id</i> <b>enum</b> <i>interface-name1</i> <i>interface-name2 ...</i> <i>interface-nameN</i> [ <b>point-to-point</b>   <b>multipoint</b> ]	Mandatory By default, the interface group is not created.
Enter the global configuration mode.	<b>configure terminal</b>	-
Create interface group by specifying range mode	<b>interface group</b> <i>group-id</i> <b>range</b> <i>start-interface-</i>	Mandatory

Step	Command	Description
	<i>name end-interface-name</i> [ <b>point-to-point</b>   <b>multipoint</b> ]	By default, the interface group is not created.

---

### Note

- The interface types in the interface group should be the same. The user can configure multiple interface groups as desired.
  - The user can configure the commands supported by all types of interfaces in the interface group, but if the interfaces covered by the interface group do not support, the commands do not take effect and there may be no error prompt. Please check whether the commands take effect by viewing the configuration.
  - If the interface group covers the logical interface and when the logical interface is deleted, the logical interface in the interface group is also deleted automatically.
- 

### 16.2.3 Configure interface status SNMP agent care level

There are actually two levels of interface UP/DOWN status in the system, one is the L2 link layer status, and the other is the L3 protocol layer (protocol) status, which can be seen with the command `show ip interface brief`. Generally, both statuses change with the physical interface UP/DOWN, but when keepalive gateway is configured on Ethernet Type interface, the L3 protocol layer status will be controlled by keepalive check status.

If SNMP agent function is enabled on the device, the network management server can obtain interface status information through public mib. Moreover, it can send interface status change information to the network management server when SNMP Trap is enabled.

By means of this function command, you can set the interface status level of SNMP agent care. By default, the interface status hierarchy of SNMP agent care is L2 link layer, but when keepalive gateway is configured on Ethernet Type interface, in order to ensure consistent linkage between the interface status presented by the network management server and the keepalive check status, you need to set the interface status level of SNMP agent care as L3 protocol layer. Therefore, in environments where keepalive check is enabled (e.g. MSTP WAN line environment), it is recommended to configure link-status-care l3.

#### Configuration Condition

None

#### Interface groups

Table 16 Configuring interface status SNMP agent care level

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure interface status network management level	<b>link-status-care { I2   I3 }</b>	Mandatory By default, the interface status SNMP agent care level is L2 link layer
Exit global configuration mode	<b>exit</b>	-

## 16.2.4 Basic Monitoring and Maintaining of Interfaces

Table 16 Basic Monitoring and Maintaining of Interfaces

Command	Description
<b>clear interface group <i>group-id</i></b>	Clear the statistics information of all interfaces in the interface group
<b>interface group <i>group-id</i> display</b>	Display all interfaces contained in the current interface group
<b>show interface group <i>group-id</i></b>	Display the information of all interfaces in the interface group

# 17 Ethernet Interface

---

## 17.1 Overview

Ethernet interface includes L2 Ethernet interface and L3 Ethernet interface.

Ethernet interface, also called L2 Ethernet interface or port, is one physical interface. It works at layer 2 in the OSI reference model-data link layer. It is mainly used to execute two basic operations:

**Data frame forwarding:** According to the MAC address (that is physical address) of the data frame, forward the data frame. Ethernet interface can only perform the L2 switching forwarding for the received packets, that is, can only receive and send the packets whose source IP and destination IP are at the same segment.

**MAC address learning:** Construct and maintain the MAC address table, used to support forwarding the data frames.

L3 Ethernet interface is one physical interface. It works at layer 3 in the OSI reference model-network layer. It is mainly used to execute following basic operations.

**Packet forwarding:** The packet is routed and forwarded according to the IP (Internet Protocol) address (ie, network address) of the packet. L3 Ethernet interface can only perform the L3 routing forwarding for the received packets, that is, can receive and send the packets whose source IP and destination IP are at the different segments.

According to the maximum rate supported by the Ethernet interface, the Ethernet interface type can be divided to the following several:

**Fastethernet:** 100M port, can be abbreviated as Fa, such as fastethernet0/1 or Fa0/1;

**Gigabitethernet:** 1000M port, can be abbreviated as Gi, such as gigabitethernet0/25 or Gi0/25;

**Tengigabitethernet:** 10 Gigabit port, can be abbreviated as Te, such as tengigabitethernet1/1 or Te1/1.

**25ge:** 25G Ethernet interface;

**40ge:** 40G Ethernet interface;

**100ge:** 100G Ethernet interface;

According to the media type of the port, the port type can be divided to copper (electrical port) and fiber (optical port).

## 17.2 Ethernet Interface Function Configuration

Table 17 Function Configuration List of Ethernet Interface

Configuration Task	
Configure Basic Functions of Port	Enter Ethernet interface configuration mode
	Enter Batch Configuration Mode of L2 Ethernet Interface
	Configure Port Rate and Duplex Mode
	Configure FEC
	Configure MDIX (Media Dependent Interface Crossover) mode
	Configure Port Media Type
	Configure MTU (Maximum Transmission Unit)
	Configure Port Flow Control
	Configure Delay Time
	Configure Port Auto Energy-Saving
	Configure Port Energy Efficient Ethernet Function
	Configure optical module type supported by the port
Configure Port Detection Function	Configure Port Status Flap Detection
	Enable Port Loopback Test
Configure Storm Suppression	Configure Storm Suppression Parameters
	Configure the action executed after the storm suppression

Configuration Task	
Configure UNI/NNI attribute	Configure UNI/NNI attribute
	Configure Connectivity of uni Port
Configure basic functions of L3 Ethernet interface	Configure L3 Ethernet interface

## 17.2.1 Configure Basic Functions of Port

### Configuration Condition

None

### Enter Ethernet interface configuration mode

To configure on the specified Ethernet interface, first enter the L2 Ethernet interface configuration mode of the Ethernet interface and then execute the corresponding configuration command.

Table 171 Enter L2 Ethernet Interface Configuration Mode

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the L2/L3 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  The subsequent configuration takes effect only on the current interface after you enter the L2/L3 Ethernet interface configuration mode

### Note

- The naming rule of the Ethernet interface number is U/S/P (Unit/Slot/Port). Unit indicates the device in stacking status, numbered from 0. When the device is initialized, it needs to be clear whether it is in the stacking status. If not, the device number defaults to 0 and is hidden.

---

Slot indicates slots on the device, numbered from 0. If there is fixed Ethernet interface, slot 0 is reserved for the fixed Ethernet interface, while service slot is numbered from 1. Port indicates Ethernet interface on each device or interface card which is numbered from 1.

- The naming rule of Ethernet interface *interface-name* is Ethernet interface type + Ethernet interface number. For example, gigabitethernet0/1 represents the gigabit Ethernet interface numbered 1; tengigabitethernet1/2 represents the 10 gigabit Ethernet interface numbered 2 on the service slot numbered 1; in stacking mode, gigabitethernet0/1/2 represents that the member number is 0, with gigabit Ethernet interface numbered 2 on the service slot numbered 1.
- 

### Enter Batch Configuration Mode of L2 Ethernet Interface

When performing the same configuration on multiple ports, to improve the configuration efficiency and reduce the repeated steps, select to enter the batch configuration mode of the L2 Ethernet interface, including the following three cases: single port, such as gigabitethernet 0/1; successive ports, using "-" to indicate one section of successive ports, such as gigabitethernet 0/3-0/5, indicating port 0/3, 0/4, and 0/5; single port and successive ports, using comma to separate them. For example, "gigabitethernet 0/1, 0/3-0/4, and 0/6" represents ports 0/1, 0/3, 0/4, and 0/6.

Table 172 Entering Batch Configuration Mode of L2 Ethernet Interface

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter Batch Configuration Mode of L2 Ethernet Interface	<b>interface interface-list</b>	Mandatory

---

#### Note

- L3 Ethernet interface does not support the batch configuration mode.
- 

### Configure Port Rate and Duplex Mode

Setting the port rate includes two cases:

One is to set the fixed rate according to the Ethernet interface rate capability set. The optional parameters include **10** (10M), **100** (100M), **1000** (1000M), **10000** (10000M), **25000** (25000M), **40000** (40000M), and **100000** (100000M);

The other is to set the rate as auto (auto-negotiation), specifying that the rate is negotiated by the local end and the peer port.

Similarly, setting the port duplex mode includes two cases:

One is to set the duplex mode according to the capability set of the port duplex mode. The optional parameters include full (full-duplex mode), indicating that the port can send packets when receiving the packets; half (half-duplex mode), indicating that the port can only receive or send packets at one moment, but cannot perform at the same time;

The other is to set the duplex mode as auto (auto-negotiation), indicating that the duplex mode is negotiated automatically by the local end and the peer port.

Table 173 Configuring Port Rate and Duplex Mode

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the L2/L3 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  The subsequent configuration takes effect only on the current interface after you enter the L2/L3 Ethernet interface configuration mode
Configure the port rate	<b>speed</b> { <b>10</b>   <b>100</b>   <b>1000</b>   <b>10000</b>   <b>25000</b>   <b>40000</b>   <b>100000</b>   <b>auto</b> }	Mandatory
Configure the port duplex mode	<b>duplex</b> { <b>auto</b>   <b>full</b>   <b>half</b> }	Mandatory

### Configure FEC

FEC (Forward Error Correction) is one error correction method that adds error correction information to the data packet at the sending port, and uses the error correction information at the receiving end to correct the error produced upon transmission of the data packet in order to improve the signal quality, but at the same time it will also bring some delay to the signal. The user can choose to enable or disable this function according to the actual situation.

The FEC status of the port can be manually configured by the user, or be configured in an adaptive manner. If the user does not configure the supported optical module type on the port, the FEC will be configured adaptively according to the type and rate of the module inserted in the current port upon inserting of the module or configuring of the port rate. If there is user configuration on the port, the user configuration will prevail, and no adaptation will be done upon inserting of the module into the port or configuring of SPEED.

Table 17-4 Configuring Port FEC Status

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the L2/L3 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  The subsequent configuration takes effect only on the current interface after you enter the L2/L3 Ethernet interface configuration mode
Configure port FEC status	<b>[no] fec mode {base-r {auto   manual}   rs { auto   manual }   none manual}</b>	Mandatory  By default, FEC is not enabled on the port

### Note

- When the rate is not 25G or 100G, it is not allowed to configure FEC. When the port has manual configuration of FEC, it is not allowed to switch the rate to other than 25G or 100G.
- This function is not allowed to be configured on VSL member port.
- The auto configuration is adaptively issued. Before restarting the device, the user needs to use the write command to save this configuration.
- Only 25GE and 100GE interfaces support this function. The fec configuration will take effect only when the actual rate is 25G or 100G.

### Configure Port MDIX Mode

You can send and receive signals only after connecting the local end and the peer port. Therefore, the MDIX mode is used with connection cables.

The cables connecting ports are divided to two types: straight-through cable and crossover cable. To support the two types of cables, provide three kinds of MDIX modes: normal, cross and auto.

The optical port can only support straight-through cable. Therefore, MDIX mode can only be set as normal.

The electrical port is formed by eight pins. You can change the roles of the pins by setting the MDIX mode. When setting as normal, use pin 1 and 2 to send signals, and pin 3, 6 to receive signals; when setting as cross, use pin 1, 2 to receive signals, pin 3, 6 to send signals; when setting as auto, the local and peer electrical ports automatically negotiate the functions of the pins by connecting the cables.

When using the straight-through cable, the MDIX modes of the local and peer ports cannot be the same.

When using crossover cable, the MDIX modes of the local and peer ports should be the same or at least one is auto.

Table 175 Configuring MDIX Mode

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the L2/L3 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  The subsequent configuration takes effect only on the current interface after you enter the L2/L3 Ethernet interface configuration mode
Configure the mode of receiving and sending signals via network cable	<b>mdix { auto   cross   normal }</b>	Mandatory  By default, the MDIX mode of the electrical port is auto and the MDIX mode of the optical port is normal.

---

 **Note**

- The Optical port does not support this configuration.
- 

### Configure Port Media Type

Switch to use the optical port or electrical port on the Combo port by configuring the port media type. The optical port and the corresponding electrical port cannot work at the same time. When specifying one type of ports on Combo port, the other type of ports are automatically disabled.

Table 176 Configuring Media Type

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the L2/L3 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  The subsequent configuration takes effect only on the current interface after you enter the L2/L3 Ethernet interface configuration mode
Configure Port Media Type	<b>media-type</b> { <b>auto</b>   <b>copper</b>   <b>fiber</b> }	Mandatory  By default, the media type of the electrical port is copper; the media type of the optical port is fiber; the media type of the Combo port is copper.

---

 **Note**

- When switching the optical port and electrical port on the Combo port, the port configuration after switching, such as rate, duplex mode, and MDIX mode, are initialized to the default values.
- 

### Configure Port MTU

The MTU configured on the port takes effect at the same time for the ingress and egress packets, and the set values are the same. When the length of the received and sent packets exceeds the set value, the packets are dropped directly.

In contrast, the MTU configured on L3 Ethernet interface only takes effect for the egress packets. When the length of the sent packet exceeds the set value, the packet first performs the IP fragmenting, making the length of the fragmented packet not exceed the set value, and then send it out.

Table 17-7 Configuring MTU

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the L2/L3 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  The subsequent configuration takes effect only on the current interface after you enter the L2/L3 Ethernet interface configuration mode
Configure Port MTU	<b>mtu</b> <i>mtu-value</i>	Mandatory  By default, the port MTU is 1824 bytes.

### Configure Port Flow Control

When the sending or receiving buffer is full and if the duplex mode of the port is half-duplex, send the blocking signals back to the source end by the back pressure mode; if the duplex mode of the port is full-duplex mode, the port informs the source end to stop sending by the flow control mode.

Table 17-8 Configuring Flow Control

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	-
Configure Port Flow Control	<b>flowcontrol { on   off }</b>	Mandatory  By default, the flow control function of the port is disabled.

---

 **Note**

- Only when the flow control function is enabled on both the local port and the peer port, can the flow control on the local port be realized.
- 

### Configure Delay Time

When the port changes from Up to Down, first enter the set suppression time period and the switching of the port status is not felt by the system; and then after the set suppression time, report the port status change to the system. In this way, you can avoid the unnecessary running cost caused by the frequent switching of the ports status in short time.

Table 179 Configuring Delay Time

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the L2/L3 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	-
Configure Delay Time	<b>link-delay</b> <i>link-delay-value</i>	Mandatory  By default, the delay report time of the port changing from Up to Down is 0, that is, disable the delay report function; when the port changes from Up to Down, report and process immediately.

### Configure Port Auto Energy-Saving

When disabling or enabling port auto energy-saving, but not connecting cables, the port inside is always in the polling port state. To reduce the unnecessary energy consumption, automatically switch to the low energy consumption state when the port is idle by configuring the port auto energy-saving.

Table 17-10 Configuring Auto Power-down

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the L2/L3 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	-
Configure Port Auto Energy-Saving	<b>auto-power-down enable</b>	Mandatory  By default, the auto energy-saving function of the port is disabled.

---

### Note

- This device does not support auto power-down configuration.
- 

### Configure Port Energy Efficient Ethernet Function

When no data traffic passes, the inner port is always polling the port state. To reduce such unnecessary consumption, you can configure the interface energy efficient Ethernet function. When the interface is idle, it is automatically switched to the low energy state. When the data is normally transmitted, recover the power supply.

Table 17-11 Configuring Energy Efficient Ethernet Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the L2/L3 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  The subsequent configuration takes effect only on the current interface after you enter the L2/L3 Ethernet interface configuration mode

Step	Command	Description
Configure Port Energy Efficient Ethernet Function	<b>energy-efficient-ethernet enable</b>	Mandatory  By default, the energy efficient Ethernet function of the interface is disabled.

---

### Note

- After the interfaces on the both sides of the cable are enabled with the energy efficient Ethernet function, the function can take effect.
  - The optical interface does not support such energy efficient Ethernet function.
  - The interface with the rate as 10 Mbps and with the duplex mode as any mode and the interface with the rate as 100 Mbps and the duplex mode not as the automatic negotiation mode do not support the energy efficient Ethernet function.
- 

### Configure optical module type supported by the port

The gigabit and 10 gigabit Ethernet optical interfaces are in OMM-disabled status when the optical module is not inserted in. This port can be enabled only when the type of the optical module inserted on the port is the same as the optical module type supported by the port configuration. Therefore, the optical module type supported by the port needs to be configured, which can be manually done by the user or done in an adaptive manner. If the user does not configure the supported optical module type on the port, the optical module type supported by the port will be adaptively configured according to the type of the module inserted on the port, so that the port can use the corresponding optical module normally. If there is user configuration on the port, the user configuration will prevail, and no adaptation will be done according to the type of the module inserted on the port.

The types of optical modules are divided into gigabit photoelectric modules, 10 gigabit photoelectric modules, ordinary optical modules, and unrecognizable-typed optical modules. Among them, the ordinary optical modules include gigabit optical modules, 10 gigabit optical modules, 10 gigabit high-speed cables, 40G optical modules, 40G high-speed cables and other optical modules. Unrecognizable optical modules offer no guarantee for normal use.

By default, the port supports ordinary optical modules.

Due to the different speed capability levels supported by different types of modules, the speed configuration of the port may be modified synchronously when the configuration port supports different optical module types (including user configuration and adaptive configuration).

Table 17-12 Configuring Optical Module Type Supported by the Port

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the L2/L3 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  The subsequent configuration takes effect only on the current interface after you enter the L2/L3 Ethernet interface configuration mode
Configure photoelectric module supported by the port	<b>optical fiber-to-copper</b> { <b>get</b>   <b>xget</b> }	Mandatory  By default, the port supports ordinary optical modules
Clear the configuration of the supported optical module type on the port	<b>no optical fiber-to-copper</b> { <b>get</b> [auto]   <b>xget</b> [auto]   <b>unknown-module auto</b> }	Mandatory  The auto command is used to clear the adaptive configuration. It cannot clear the user configuration. After the adaptive configuration is cleared, the port supports ordinary optical modules by default. In this case, you need to unplug or plug the optical module or restart the device to trigger again the adaptation.  The non-auto command is used to clear the user configuration. The optical module inserted on the port will be automatically re-adapted according to the type of this optical module.



## Note

- This function is only allowed to be configured on the Ethernet optical interface, and not allowed to be configured on the electrical port and the combo port.
- This function is not allowed to be configured on VSL member port.
- This function is not allowed to be configured on 40G and 100G ports.
- The auto configuration is adaptively issued. Before restarting the device, the user needs to use the write command to save this configuration.

### Configure mandatory cancel of interface OMM-disabled status

If the optical module is not inserted on the Ethernet optical interface, the port will be in the OMM-disabled status and cannot receive and send packets. After inserting of the legal optical module, the OMM-disabled status of the Ethernet optical interface will be automatically canceled. But, sometimes the Ethernet port needs to be UP without the optical module inserted, such as enabling the loopback check function. In this case, you can configure to mandatorily cancel the OMM-disabled status of the Ethernet optical interface.

The Ethernet optical interface will be in the OMM-disabled status only when it has no optical module inserted. The electrical interface and Combo interface will not be set to the OMM-disabled status, and therefore, this function is not required.

Table 17-13 Enabling Mandatory Cancel of Interface OMM-disabled Status/Disabling Mandatory Cancel of Interface OMM-disabled Status

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the L2/L3 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  The subsequent configuration takes effect only on the current interface after you enter the L2/L3 Ethernet interface configuration mode
Enable mandatory cancel of interface OMM-disabled status	<b>optical enable port manual</b>	Mandatory  By default, this function is disabled

Step	Command	Description
Disable mandatory cancel of interface OMM-disabled status	<b>no optical enable port manual</b>	Mandatory By default, this function is disabled

## Note

- This function is only allowed to be configured on the Ethernet optical interface, and not allowed to be configured on the electrical port and the combo port.
- This function is not allowed to be configured on VSL member port.

### Configure Port crc Error Packet Inspection Function

You need to configure `snmp-server enable traps crc-error` first. This function is used to count whether the crc error packets within the *time-value* time range exceed the max limit. If they exceed the max limit, an alarm trap will be sent. Within the *time-value* time range, when the number of crc error packets recovers from higher than the max limit to lower than the min limit, a recovery trap will be sent.

Table 17-14 Configuring crc Error Packet Inspection Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter L2 Ethernet interface configuration mode/aggregation group configuration mode	<b>interface</b> <i>interface-name</i>	Mandatory The subsequent configuration takes effect only on the current interface after you enter the L2 Ethernet interface configuration mode
Configure crc error packet inspection trap function	<b>crc-error max-limit</b> max-value <b>min-limit</b> min-value <b>interval</b> <i>time-value</i>	Mandatory By default, the function of issuing the trap when crc error packet statistics of the port exceeds the alarm range is disabled.

Step	Command	Description
		<p>max-value: The max value of the number of crc error packets of the port.</p> <p>min-value: The min value of the number of crc error packets of the port.</p> <p>time-value: Set the inspection time range, in seconds, 's'.</p>
Disable the crc error packet inspection trap function	<b>no crc-error</b>	<p>Mandatory</p> <p>By default, this function is disabled</p>

### Note

- This function takes effect only on the L2 port

### Configure Port Error Packet Inspection Function

You need to configure snmp-server enable traps { in-packet-error | out-packet-error } first. This function is used to count whether the port error packets within the *time-value* time range exceed the max limit. If they exceed the max limit, an alarm trap will be sent. Within the *time-value* time range, when the number of port error packets recovers from higher than the max limit to lower than the min limit, a recovery trap will be sent.

Table 17-15 Configuring Error Packet Inspection Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter L2 Ethernet interface configuration mode/aggregation group configuration mode	<b>interface</b> <i>interface-name</i>	<p>Mandatory</p> <p>The subsequent configuration takes effect only on the current interface after you enter</p>

Step	Command	Description
		the L2 Ethernet interface configuration mode
Configure error packet inspection trap function	<b>packet-error {in-packet   out-packet} max-limit <i>max-value</i> min-limit <i>min-value</i> interval <i>time-value</i></b>	<p>Mandatory</p> <p>By default, the function of issuing the trap when error packet statistics of the port exceeds the alarm range is disabled.</p> <p><b>in-packet</b> : Enable the trap function for the number of error in-packets of the port.</p> <p><b>out-packet</b> : Enable the trap function for the number of error out-packets of the port.</p> <p>max-value: The max value of error packets of the port.</p> <p>min-value: The min value of error packets of the port.</p> <p>time-value: Set the inspection time range, in seconds, 's'.</p>
Disable the error packet inspection trap function	<b>no packet-error {in-packet   out-packet}</b>	<p>Mandatory</p> <p>By default, this function is disabled</p>

---

### Note

- This function takes effect only on the L2 port
- 

### Configure Port Traffic Ultra-Bandwidth Function

You need to configure snmp-server enable traps {in-usage-rate | out-usage-rate } first. This function is used to send an alarm trap when the bandwidth in-usage-rate/out-usage-rate of the port exceeds the max limit. When the bandwidth in-usage-rate/out-usage-rate of the port recovers from higher than the max limit to lower than the min limit, a recovered trap will be sent.

Table 17-16 Configuring Traffic Ultra-Bandwidth Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter L2 Ethernet interface configuration mode/aggregation group configuration mode	<b>interface</b> <i>interface-name</i>	Mandatory  The subsequent configuration takes effect only on the current interface after you enter the L2 Ethernet interface configuration mode
Configure traffic ultra-bandwidth trap function	<b>flow-warn { in-packet   out-packet } max-usage max-value min-usage min-value</b>	Mandatory  By default, the traffic ultra-bandwidth trap sending function of the port is disabled.  <b>in-packet</b> : Enable the trap function for the in-usage-rate of the port.  <b>out-packet</b> : Enable the trap function for the out-usage-rate of the port.  <i>max-value</i> : The max value of bandwidth usage rate.  <i>min-value</i> : The min value of bandwidth usage rate.
Disable the traffic ultra-bandwidth trap function	<b>no flow-warn {in-packet   out-packet}</b>	Mandatory  By default, this function is disabled

 **Note**

- This function takes effect only on the L2 port

Port splitting can split one high-bandwidth physical port on the device into multiple mutually independent low-bandwidth ports. For example, the 40G port is split into 4 10G ports. The user can freely choose to use the original high-bandwidth port or split it into multiple low-bandwidth ports according to the specific type of the docking device port, which increases networking flexibility and reduces user purchase costs.

Table 17-17 Configuring Port Splitting

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	Mandatory The subsequent configuration takes effect only on the current interface after you enter the L2 Ethernet interface configuration mode
Configure port splitting	<b>split into 10GE</b>	Mandatory By default, the Ethernet interface is not split

Table 17-18 Configuring Port Merging

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name:num</i>	Mandatory The subsequent configuration takes effect only on the current interface after you enter the L2 Ethernet interface configuration mode that is optionally split
Configure port merging	<b>no split</b>	Mandatory By default, the Ethernet interface that is split is not merged

---

 **Note**

- This function takes effect only on the L2 port
- 

### Configure Port Single-Fiber Function

Configure the single-fiber function of the Ethernet interface. This function configures the Ethernet interface to only transmit packets, only receive packets, or support both transmitting and receiving packets in the single-fiber mode.

Table 17-19 Configuring Port Single-Fiber Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the L2/L3 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	Mandatory The subsequent configuration takes effect only on the current interface after you enter the L2 Ethernet interface configuration mode
Configure single-fiber function	<b>single-fiber { mode [ receive   transmit ] }</b>	Mandatory By default, the single-fiber function of the Ethernet interface is disabled. <b>mode:</b> Enable both the single-fiber transmitting and receiving functions. <b>transmit:</b> Enable the single-fiber transmitting function. <b>transmit:</b> Enable the single-fiber receiving function too.
Disable the single-fiber function	<b>no single-fiber { mode [ receive   transmit ] }</b>	Mandatory By default, this function is disabled

---

 **Note**

- This function takes effect only when the Ethernet interface is the optical interface
- 

## 17.2.2 Configure Port Detection Function

### Configure Port Status Flap Detection

When the port changes from Down to Up and if the port status flap detection is configured and it meets the detection condition, it is regarded that the status flap happens to the specified port or called Link-Flap and the port is automatically disabled and set as Error-Disabled.

Table 17-20 Configuring Port Inspection Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure port flap detection	<b>errdisable flap-setting cause link-flap max-flaps <i>max-flaps-number</i> time <i>time-value</i></b>	Mandatory By default, the trigger condition of executing Link-Flap is: within 10s, the detected port becomes Up for at least 5 times.

---

 **Note**

- When the port is disabled by the Link-Flap function and set as Error-Disabled and if it is necessary to recover automatically, you can configure the command **errdisable recovery cause** to set the above function.
- 

### Enable Port Loopback Test

When performing some troubleshooting, such as locating the port fault initially, you can enable the port loopback test function. The port enabled with the loopback test function cannot forward packets normally.

The port loopback test function includes internal loopback test and external loopback test.

During internal loopback test, change the internal receiving end and sending end of the specified port to make the packets sent by the port loopback in the device and received by the port. If the internal loopback test succeeds, it indicates that the port inside works normally. The Ethernet optical interface will be in the OMM-disabled status when the optical module is not inserted, and the internal loopback is configured not to be able to UP. In this case, you need to cancel the OMM-disabled status of the port first.

During the external loopback test, first insert one self-loop cable on the port and the packets sent by the specified port return to the port via the self-loop cable and received by the port. If the external loopback test succeeds, it indicates that the port works normally.

Table 17-21 Enabling Loopback Test

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the L2/L3 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  The subsequent configuration takes effect only on the current interface after you enter the L2/L3 Ethernet interface configuration mode
Enable Port Loopback Test	<b>loopback { internal   external }</b>	Mandatory  By default, the loopback test function for the Ethernet interface is not enabled

---

 **Note**

- The loopback test function cannot be enabled on the Ethernet interface that is shut down.
  - **loopback** command is Ethernet interface test command and will not be saved in the startup configuration file.
- 

### 17.2.3 Configure Storm Suppression

#### Configure Storm Suppression Parameters

Limit the broadcast, multicast or unknown unicast traffic on the port by configuring the storm suppression parameters. When the broadcast, multicast or unknown unicast traffic on the port exceeds the set threshold, the system drops the excessive packets, so as to make the proportion of the broadcast, multicast or unknown unicast traffic on the port reduce to the limited range and ensure the normal running of the network services.

Table 1722 Configuring Storm Suppression Parameters

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	-
Configure Storm Suppression Parameters	<b>storm-control</b> { <b>broadcast</b>   <b>multicast</b>   <b>unicast</b> } { <i>percent-value</i>   <b>kpbs</b> <i>bps-value</i>   <b>pps</b> <i>pps-value</i> }	Mandatory  By default, unicast is at 3000pps, multicast is at 3000pps, and broadcast is at 400pps

---

 **Note**

- The L3 Ethernet interface does not support the configuration of storm suppression.
- 

### Configure Action Executed after Storm Suppression

When the storm is detected on the specified port and the storm suppression is enabled, you can select three policies to process the storms on the port:

One is to make recording on the device and to print on the terminal and output the alarm information of detecting storm. In this mode, the port is enabled, so the port can receive the subsequent traffic and the storm on the port cannot be removed.

One is to disable the port, to make recording on the device and print on the terminal and output the alarm information of storm being detected, and to transmit the alarm information of the storm being detected and shutting down the port to the configured log server via trap. In this mode, the port is disabled, so the port cannot receive the subsequent traffic and the storm on the port is removed at once.

The other is to make recording on the device, to print on the terminal and output the alarm information of detecting storm, and to transmit the alarm information of detecting the storm to the configured log server

via trap. In this mode, the port is enabled, so the port can receive the subsequent traffic and the storm on the port cannot be removed.

Table 17-23 Configuring Action Executed after the Storm Suppression

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	-
Configure the action executed after the storm suppression	<b>storm-control action</b> { <b>shutdown</b>   <b>trap</b>   <b>logging</b> }	Mandatory  By default, the action executed after the storm is detected by the port is the recording on the device, and the alarm information of detecting the storm is printed on the terminal and output

---

 **Note**

- When the port is disabled by the storm suppression function and set as Error-Disabled status and if it is necessary to recover automatically, you can configure the command **errdisable recovery cause** to set the above function.
  - The L3 Ethernet interface does not support configuring the action executed after the storm suppression.
- 

## 17.2.4 Configure Port UNI/NNI Type

### Configure Port UNI/NNI Type

Uni port is the connection port between the user device and a network; nni port is the connection interface between networks. On one device, the nni port and uni port or nni ports are interconnected with no isolation; uni ports are isolated from each other.

Table 17-24 Configuring UNI/NNI Attribute

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Configure UNI/NNI attribute	<b>port-type { nni   uni }</b>	Mandatory  By default, the UNI/NNI type of the L2 Ethernet interface and aggregation group is <b>nni</b>

---

### Note

- The L3 Ethernet interface does not support the UNI/NNI type.
- 

### Configure Connectivity of uni Port

By default, all uni ports of one device are isolated from each other. However, to realize the intercommunication between the specified multiple uni ports, but not change the isolation relation between these uni ports and other uni ports, you can configure the connectivity of the uni port.

When configuring the connectivity on the specified uni port, you can only set whether the uni port can forward packets to other uni ports, without affecting whether other uni ports can forward packets to the specified uni port. Therefore, to realize the intercommunication between the multiple uni ports, you should configure as community on these uni ports separately.

Table 17-25 Configuring the Connectivity of uni Port

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected. After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Configure Connectivity of uni Port	<b>uni-isolate { community   isolated }</b>	Mandatory By default, the uni port cannot forward packets to other uni ports

---

### Note

- This command can take effect only on the uni port.
  - The L3 Ethernet interface does not support the configuration of the connectivity of the uni port.
- 

## 17.2.5 Configure basic functions of L3 Ethernet interface

The Ethernet interface processes the data packets at different levels, so it can work in the L2 mode or L3 mode. If the working mode of the Ethernet interface is set as L2 mode, it will be used as one L2 Ethernet interface; if the working mode of the Ethernet interface is set as L3 mode, it will be used as one L3 Ethernet interface, and its role is equivalent to VLAN interface. The L3 mode is divided into normal L3 mode and L3 mode with vlan reserved.

### Configuration Condition

None

### Configure Reserved vlan

Table 17-26 Configuring Reserved vlan

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure Reserved vlan	<b>vlan reserved for routedport</b> <i>vlan-list</i>	<i>vlan-list</i> : The value range is 2 to 4094  By default, no reserved vlan is created

### Configure L3 Ethernet interface

Table 17-27 Configuring L3 Ethernet Interface

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the L2/L3 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	-
Configure L3 Ethernet interface	<b>no switchport</b> <b>[reserved-vlan]</b>	Mandatory  reserved-vlan: interface mode of reserved vlan  By default, the Ethernet interface works in L2 mode and is used as one L2 Ethernet interface
Enter L3 Ethernet sub-interface configuration mode	<b>interface</b> <i>interface-name</i>	Mandatory  To enter the L3 Ethernet sub-interface configuration mode, you need to create the corresponding L3 Ethernet interface first

Step	Command	Description
		By default, there is no L3 Ethernet sub-interface

## Note

- After the working mode of the Ethernet interface is switched, all the configurations of the Ethernet interface except the description, shutdown, speed, duplex, media-type, mdix, and eee configurations will be restored to the default configuration in a new mode.
- When the Ethernet interface is used as one L3 interface, please refer to the configuration of the basic functions of the VLAN interface for the configuration of the basic functions of the L3 Ethernet interface.
- To switch the L2 Ethernet interface to the L3 Ethernet interface of the reserved vlan, you need to create the reserved vlan first.
- The L3 Ethernet interface of the reserved vlan is used only in vxlan environment.
- To switch between the ordinary L3 interface and the L3 interface of the reserved vlan, you need to switch to the L2 interface first, and then to the required L3 interface mode.

## 17.2.6 Ethernet Interface Monitoring and Maintaining

Table 17-28 Ethernet Interface Monitoring and Maintaining

Command	Description
<b>clear interface</b> <i>interface-name</i>	Clear the statistics information of the specified L3 Ethernet interface
<b>clear interface</b> { <i>interface-list</i>   <b>switchport</b> } <b>statistics</b>	Clear the packet and traffic statistics information of the port
<b>clear optical</b> { <b>all</b>   <b>interface</b> <i>interface-list</i> } <b>exception statistic</b>	Clear the exception statistics information of the optical module inserted on the Ethernet interface
<b>show errdisable flap-values</b>	Display the current setting of triggering executing Link-Flap function
<b>show interface</b> { <i>interface-list</i> [ <b>group</b> ]   <b>switchport</b> [ <b>brief</b> [ <b>down</b>   <b>up</b>   <b>vsl</b> ] ] }	Display all information or abstract information of the Ethernet interface or virtual switch link member port

Command	Description
<b>show interface <i>interface-list</i> statistics</b>	Display the packet and traffic statistics information of the port
<b>show interface switchport statistics</b> [ <b>packet</b>   <b>rate</b>   <b>ratio</b> ]	Display the packet and traffic statistics information of all ports on the device
<b>show interface all statistics</b> [ <b>packet</b>   <b>rate</b>   <b>ratio</b> ]	Display the packet and traffic statistics information of all L2 interfaces and L3 interfaces on the device
<b>show optical</b> { <b>all</b>   <b>interface <i>interface-list</i></b> } [ <b>detail</b>   <b>exception statistic</b> ]	Display the information of the optical module inserted on the Ethernet interface
<b>show port-type</b> [ <i>interface-list</i>   { <b>uni</b>   <b>nni</b> } [ <b>interface <i>interface-list</i></b> ] ]	Display the UNI/NNI attribute information of the port
<b>show group-port</b>	Display the attribute information of the same group that the Ethernet interfaces belong to
<b>show interface <i>interface-list</i> rate-peak</b> [ <b>input</b> / <b>output</b> ]	Display the traffic monitoring information of the specified port
<b>show storm-control</b> [ <b>interface <i>interface-list</i></b> ]	Display the storm suppression setting of the specified port
<b>show optical</b> { <b>all</b>   <b>interface <i>interface-list</i></b> } <b>omm-disabled status</b>	Display whether the port is in OMM-disabled status and the reason why the port is in the OMM-disabled status
<b>show routedport reserved-vlan</b>	Display the usage of reserved vlan

## 17.3 Typical Configuration Example of Ethernet Interface

### 17.3.1 Configure Storm Suppression Function

#### Network Requirements

- Configure the storm suppression function on the port of the device to suppress the broadcast, unknown unicast and multicast packets, realizing that PC2 can access Internet normally when PC1 sends lots of broadcast, unknown unicast and multicast packets.

## Network Topology

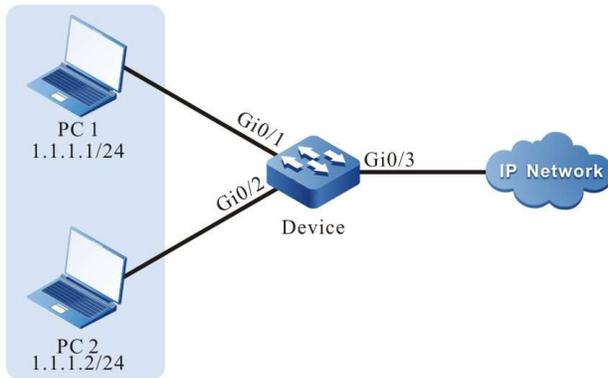


Figure 17-1 Configuring Network Topology of Storm Suppression

## Configuration Steps

*Step 1:* Configure VLAN and port link type on Device.

# Create VLAN2 on Device.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the link type of port gigabitethernet0/1 and gigabitethernet0/2 on Device as Access, permitting the services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/1,0/2
Device(config-if-range)#switchport mode access
Device(config-if-range)#switchport access vlan 2
Device(config-if-range)#exit
```

#Configure the link type of port gigabitethernet0/3 on Device as Trunk, permitting the services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/3
Device(config-if-gigabitethernet0/3)#switchport mode trunk
Device(config-if-gigabitethernet0/3)#switchport trunk allowed vlan add 2
Device(config-if-gigabitethernet0/3)#exit
```

*Step 2:* Configure the storm suppression function

#Adopt bps limitation mode to suppress the broadcast, unknown unicast and multicast packets on port gigabitethernet0/1 and the suppression rate is 1024Kbps.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#storm-control broadcast kbps 1024
Device(config-if-gigabitethernet0/1)#storm-control unicast kbps 1024
Device(config-if-gigabitethernet0/1)#storm-control multicast kbps 1024
Device(config-if-gigabitethernet0/1)#exit
```

*Step*  
3:

Check the result.

#View the storm suppression information of port gigabitethernet0/1 on Device.

```
Device#show storm-control interface gigabitethernet 0/1
Status Codes: U - unicast, B - broadcast, M - multicast
Interface      Unicast  Broadcast  Multicast  Action  Status
-----
gi0/1          1024kbps 1024kbps  1024kbps  logging -|-
```

#When PC1 sends lots of broadcast, unknown unicast and multicast packets, PC2 also can access Internet normally.

# 18 Aggregation Group Interface

## 18.1 Overview

Aggregation group interface is one logical interface, including L2 aggregation group interface and L3 aggregation group interface. When enabling the link aggregation function on multiple ports, the multiple ports with the same link aggregation feature form the aggregation group and are abstracted to aggregation group interface; meanwhile, the multiple ports with the same attribute are called the member ports of the aggregation group. It is mainly used to expand the link bandwidth and improve the connection reliability.

## 18.2 Aggregation Group Interface Function Configuration

Table 18-1 Function Configuration List of Aggregation Group Interface

Configuration Task	
Configure Basic Functions of Aggregation Group Interface	Enter the aggregation group interface configuration mode

### 18.2.1 Configure basic functions of L3 aggregation group interface

#### Configuration Condition

None

#### Configure Reserved vlan

Table 182- Configuring Reserved vlan

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Configure Reserved vlan	<b>vlan reserved for routedport</b> <i>vlan-list</i>	<i>vlan-list</i> : The value range is 2 to 4094  By default, no reserved vlan is created

### Configure L3 Aggregation Group Interface

Table 18-3 Configuring L3 Aggregation Group Interface

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the L2/L3 aggregation group interface configuration mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	Mandatory
Configure L3 Aggregation Group Interface	<b>no switchport</b> <b>[reserved-vlan]</b>	Mandatory  reserved-vlan: interface mode of reserved vlan  By default, the aggregation Ethernet interface works in L2 mode and is used as one L2 Ethernet aggregation interface
Enter L3 aggregation group sub-interface configuration mode	<b>interface</b> <i>interface-name</i>	Mandatory  To enter the L3 aggregation group sub-interface configuration mode, you need to create the corresponding L3 aggregation interface first  By default, there is no L3 aggregation group sub-interface

---

## Note

- Before entering the specified aggregation group interface configuration mode, you must first create the corresponding aggregation group.
  - After the working mode of the aggregation group interface is switched, all the configurations of the aggregation group interface except the description and shutdown configurations will be restored to the default configuration in a new mode.
  - When the aggregation group interface is used as one L3 interface, please refer to the configuration of the basic functions of the VLAN interface for the configuration of the basic functions of the L3 Ethernet interface.
  - To switch the L2 aggregation group interface to the L3 aggregation group interface of the reserved vlan, you need to create the reserved vlan first.
  - The L3 aggregation interface of the reserved vlan is used only in vxlan environment.
  - To switch between the ordinary L3 interface and the L3 interface of the reserved vlan, you need to switch to the L2 interface first, and then to the required L3 interface mode.
- 

## 18.2.2 Monitoring and Maintaining of Aggregation Group Interface

Table 18-4 Monitoring and Maintaining of Aggregation Group Interface

Command	Description
<b>clear interface link-aggregation</b> <i>link-aggregation-id</i>	Clear the statistics information of the specified L3 aggregation group interface
<b>clear interface switchport link-aggregation</b> <i>link-aggregation-id</i> <b>statistics</b>	Clear the packet and traffic statistics information of the specified L2 aggregation group
<b>show interface switchport link-aggregation</b> [ <b>brief</b>   <b>description</b> ]	Display all information or description information of the L2 aggregation group
<b>show interface link-aggregation</b> <i>link-aggregation-id</i> <b>statistics</b>	Display the packet and traffic statistics information of the specified aggregation group
<b>show interface link-aggregation</b> <i>link-aggregation-id</i> <b>rate-peak</b> [ <b>input</b>   <b>output</b> ]	Display the traffic monitoring information of the specified aggregation group
<b>show port-type interface link-aggregation</b> <i>link-aggregation-id</i>	Display the UNI/NNI attribute information of the L2 aggregation group

# 19 VLAN Interface

---

## 19.1 Overview

VLAN interface is one logical interface, used to be bound with VLAN and complete the packet forwarding between different VLANs. One VLAN can only be bound to one VLAN interface. One VLAN interface also can only be bound with one VLAN.

## 19.2 VLAN Interface Function Configuration

Table 19-1 VLAN Interface Function Configuration List

Configuration Task	
Configure the basic functions of the VLAN interface	Configure VLAN interface
	Configure the logical bandwidth of the interface
	Configure interface delay
	Configure interface MTU
	Configure interface protocol delay UP

### 19.2.1 Configure the basic functions of the VLAN interface

#### Configuration Condition

None

#### Configure VLAN interface

Table 19-2 Configuring VLAN Interface

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Create VLAN interface	<b>interface vlan <i>vlan-id</i></b>	Mandatory  By default, do not create VLAN interface.

### Note

- VLAN interface is one logical interface. To work normally, you need to create the corresponding VLAN and add the physical port to VLAN. For how to create VLAN and add physical ports to the VLAN, refer to the related chapters in the User Manual VLAN.
- There is no order requirement for creating VLAN interface, creating VLAN and adding physical port to VLAN.

### Configure the logical bandwidth of the interface

The logical bandwidth of the interface affects the calculation of the route cost and QoS, but does not affect the physical bandwidth of the interface. Usually, when the interface is connected to WAN, it is suggested that the logical bandwidth of the user configuration interface is consistent with the actual bandwidth of the leased line.

Table 19-3 Configuring Logical Bandwidth of Interface

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface vlan <i>vlan-id</i></b>	-
Configure the logical bandwidth of VLAN interface	<b>bandwidth <i>width-value</i></b>	Optional  By default, the logical bandwidth of the VLAN interface is 100,000 Kbps.

### Configure interface delay

The interface delay configuration affects the calculation of the routing protocol cost, but does not affect the actual transmission delay of the interface. The user can change the cost of the routing protocol by configuring the interface delay.

Table 19-4 Configuring Interface Delay

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface vlan <i>vlan-id</i></b>	-
Configure VLAN interface delay	<b>delay <i>delay-time</i></b>	Optional By default, the delay of the VLAN interface is 10 and the unit is 10 microsecond.

### Configure interface MTU

The interface MTU decides the maximum length of the IP fragment packet and the user can configure manually.

Table 19-5 Configuring Interface MTU

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface vlan <i>vlan-id</i></b>	-
Configure VLAN interface MTU	<b>mtu <i>mtu-size</i></b>	Mandatory By default, the VLAN interface MTU is 1500 bytes.

### Configure interface protocol delay UP

UP and DOWN of the interface can be specifically divided into UP/DOWN of the link and UP/DOWN of the protocol; after the link is UP, the system informs the upper layer protocol module and other modules through the protocol UP to start transmitting and receiving packets.

In some cases (such as device restart or monoboard reset, etc.), when the link status of the interface changes from DOWN to UP, the upper-layer protocol module may not be ready and cannot process packets temporarily; at this point, the interface protocol delay UP can be configured, and the interface is delayed for a certain period of time to notify the protocol UP again.

Table 19-6 Configuring Interface Protocol Delay UP

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface vlan <i>vlan-id</i></b>	-
Configure VLAN interface protocol delay UP	<b>protocol up-delay-time <i>delay-seconds</i></b>	Mandatory  By default, the time of the VLAN interface protocol delay UP is 0

## 19.2.2 VLAN Interface Monitoring and Maintaining

Table 19-7 VLAN Interface Monitoring And Maintaining

Command	Description
<b>clear interface vlan <i>vlan-id</i></b>	Clear the statistics information of the specified VLAN interface
<b>show interface vlan <i>vlan-id</i></b>	View the information of the specified VLAN interface
<b>show interface vlan <i>vlan-id</i> original statistics</b>	View the statistics information of the specified VLAN interface

## 19.3 Typical Configuration Example of VLAN Interface

### 19.3.1 Configure VLAN interface

#### Network Requirements

- Configure the VLAN interface on Device to realize the intercommunication between PC1 and PC2 of different VLANs.

#### Network Topology

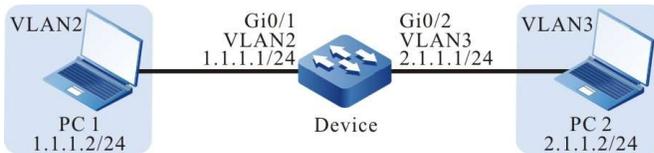


Figure 19-1 Configuring Network Topology of VLAN Interface

#### Configuration Steps

*Step 1:* Configure VLAN and port link type on Device.

#Create VLAN2 and VLAN3 on Device.

```
Device#configure terminal
Device(config)#vlan 2-3
```

#Configure the link type of port gigabitethernet0/1 and gigabitethernet0/2 on Device as Access. Port gigabitethernet0/1 permits the services of VLAN2 to pass and gigabitethernet0/2 permits the services of VLAN3 to pass.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode access
Device(config-if-gigabitethernet0/1)#switchport access vlan 2
Device(config-if-gigabitethernet0/1)#exit
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode access
Device(config-if-gigabitethernet0/2)#switchport access vlan 3
Device(config-if-gigabitethernet0/2)#exit
```

*Step 2:* Configure the VLAN interface and IP address on Device.

#Create VLAN2 interface on Device whose IP address is 1.1.1.1 and subnet mask is 255.255.255.0; create VLAN3 interface whose IP address is 2.1.1.1 and subnet mask is 255.255.255.0.

```
Device(config)#interface vlan 2
Device(config-if-vlan2)#ip address 1.1.1.1 255.255.255.0
Device(config-if-vlan2)#exit
Device(config)#interface vlan 3
Device(config-if-vlan3)#ip address 2.1.1.1 255.255.255.0
Device(config-if-vlan3)#exit
```

Step  
3:

Check the result.

#View the information of VLAN interface on Device.

```
Device#show interface vlan 2
vlan2:
  line protocol is up
  Flags: (0xc008063) BROADCAST MULTICAST ARP RUNNING
  Type: ETHERNET_CSMACD
  Internet address: 1.1.1.24
  Broadcast address: 1.1.1.255
  Metric: 0, MTU: 1500, BW: 100000 Kbps, DLY: 100 usec, VRF: global
  Reliability 255/255, Txload 1/255, Rxload 1/255
  Ethernet address is 0012.2355.9913
  5 minutes input rate 0 bits/sec, 0 packets/sec
  5 minutes output rate 0 bits/sec, 0 packets/sec
  0 packets received; 1 packets sent
  0 multicast packets received
  1 multicast packets sent
  0 input errors; 0 output errors
  0 collisions; 0 dropped
  Unknown protocol 0
Device#show interface vlan 3
vlan3:
  line protocol is up
  Flags: (0xc008063) BROADCAST MULTICAST ARP RUNNING
  Type: ETHERNET_CSMACD
  Internet address: 2.1.1.24
  Broadcast address: 2.1.1.255
  Metric: 0, MTU: 1500, BW: 100000 Kbps, DLY: 100 usec, VRF: global
  Reliability 255/255, Txload 1/255, Rxload 1/255
  Ethernet address is 0012.2355.9913
  5 minutes input rate 0 bits/sec, 0 packets/sec
  5 minutes output rate 0 bits/sec, 0 packets/sec
  0 packets received; 1 packets sent
  0 multicast packets received
  1 multicast packets sent
  0 input errors; 0 output errors
  0 collisions; 0 dropped
  Unknown protocol 0
```

#PC1 can ping PC2.

# 20 Loopback Interface

---

## 20.1 Overview

Loopback interface, also called local loopback interface, is logical virtual interface implemented by software. This interface is not affected by the physical status. As long as it is not manually disabled, its status is always enabled status. In dynamic routing protocols such as OSPF, you can select the IP address of the Loopback interface as the Router ID, as the identifier of the device. For packets sent to the Loopback interface, the device considers each packet to be sent to itself and will not forward the packet.

## 20.2 Loopback Interface Function Configuration

Table 20-1 Loopback Interface Function Configuration List

Configuration Task	
Configure the basic functions of the Loopback interface	Configuring the Loopback interface
	Configure the logical bandwidth of the interface
	Configure interface delay

### 20.2.1 Configure the basic functions of the Loopback interface

#### Configuration Condition

None

#### Configuring the Loopback interface

Table 20-2 Configuring Loopback Interface

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Create Loopback interface	<b>interface loopback</b> <i>unit – number</i>	Mandatory  By default, no Loopback interface is created

### Configure the logical bandwidth of the interface

The logical bandwidth of the interface affects the calculation of the route cost and QoS, but does not affect the physical bandwidth of the interface. Usually, when the interface is connected to WAN, it is suggested that the logical bandwidth of the user configuration interface is consistent with the actual bandwidth of the leased line.

Table 20-3 Configuring Logical Bandwidth of Interface

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure the logical bandwidth of the interface	<b>bandwidth</b> <i>width-value</i>	Optional  By default, the logical bandwidth of the Loopback interface is 8,000,000 Kbps

### Configure interface delay

The interface delay configuration affects the calculation of the routing protocol cost, but does not affect the actual transmission delay of the interface. The user can change the cost of the routing protocol by configuring the interface delay.

Table 20-4 Configuring Interface Delay

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure interface delay	<b>delay</b> <i>delay-time</i>	Optional By default, the delay of the Loopback interface is 5000, in 10 microseconds

# 21 Null Interface

---

## 21.1 Overview

Null interface is logical virtual interface implemented by software. Any packet sent to the Null interface will be dropped. Dynamic routing protocols such as OSPF will generate automatically summarized routes, and the outlet interface points to the Null interface, which can effectively avoid routing loops. The Null 0 interface is created by the device by default and cannot be disabled or deleted by the user.

## 21.2 Null Interface Function Configuration

Table 21-1 Null Interface Function Configuration List

Configuration Task	
Configure the Basic Functions of the Null Interface	Configure the Basic Functions of the Null Interface

### 21.2.1 Configure the Basic Functions of the Null Interface

#### Configuration Condition

None

#### Configure the Basic Functions of the Null Interface

Table 21-2 Configuring Basic Functions of Null Interface

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter Null interface configuration mode	<b>interface null 0</b>	Mandatory
Configure to prohibit transmit ICMP unreachable error packets	<b>no ip unreachable</b>	Optional By default, transmitting ICMP unreachable error packets is prohibited

---

### Note

- The Null interface only supports the configuration of allowing or prohibiting transmitting of ICMP unreachable error packets.
  - Packets reaching the Null interface will be dropped, you have no need to transmit ICMP unreachable errors.
-

# 22 Virtual Switch Link Interface

## 22.1 Overview

By binding multiple physical ports together, one virtual switch link interface (VSL-Channel) can be formed. The virtual switch link interface is logical link channel for protocol packet interaction and service data forwarding between member switches in the stack system, and each physical port therein is called member port of the virtual switch link.

Each member switch joins the same switch domain, interconnects with each other through the virtual switch link interface, and finally forms one virtual switch.

## 22.2 Virtual Switch Link Interface Function Configuration

Table 22-1 Virtual Switch Link Interface Function Configuration List

Configuration Task	
Configure functions of the virtual switch link interface	Enter virtual switch link interface configuration mode

### 22.2.1 Configure functions of the virtual switch link interface

#### Configuration Condition

None

#### Enter virtual switch link interface configuration mode

Table 22-2 Entering Virtual Switch Link Interface Configuration Mode

Step	Command	Description
Enter the global configuration mode.	configure terminal	-

Step	Command	Description
Enter virtual switch link interface configuration mode	<code>vsl-channel vsl-channel-id</code>	Mandatory  In stand-alone mode, <i>vsl-channel-id</i> is a one-dimensional value that represents a virtual switch link interface number. In stack mode, it is a two-dimensional value. The first dimension is a virtual switch member number, and the second dimension is a virtual switch link interface number

---

### Note

- Before entering the virtual switch link interface configuration mode, you must first create the corresponding virtual switch link interface.
- 

## 22.2.2 Monitoring and Maintaining of Virtual Switch Link Interface

Table 22-3 Monitoring and Maintaining of Virtual Switch Link Interface

Command	Description
<b>clear vsl-channel vsl-channel-id statistics</b>	Clear the packet and traffic statistics information of the specified virtual switch link interface
<b>show vsl-channel vsl-channel-id rate-peak [ input   output ]</b>	Display the traffic monitoring information of the specified virtual switch link interface
<b>show vsl-channel vsl-channel-id statistics</b>	Display the packet and traffic statistics information of the specified virtual switch link interface

# 23 Tunnel Interface

## 23.1 Overview

Tunnel is one technology that uses one network protocol to transmit another network protocol. It includes the entire process of data encapsulation, transmission, and decapsulation. The path through which the encapsulated packets are transmitted in the network is called Tunnel. Tunnel is one virtual point-to-point connection. The devices at both ends of Tunnel are called Tunnel endpoints, and they are responsible for encapsulating and decapsulating data packets.

## 23.2 Tunnel Interface Function Configuration

Table 23-1 Tunnel Interface Function Configuration List

Configuration Task	
Configure the basic functions of the Tunnel interface	Configure the basic functions of the Tunnel interface

### 23.2.1 Configure the basic functions of the Tunnel interface

#### Configuration Condition

None

#### Configure Basic Functions of Tunnel Interface

Table 23-2 Configuring Basic Functions of Tunnel Interface

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Create Tunnel interface and enter its configuration mode	<b>interface tunnel</b> <i>tunnel-unit</i>	Mandatory By default, no Tunnel interface is created on the device
Configure the working mode of the Tunnel interface	<b>tunnel mode</b> { <i>gre</i> [ <i>ip</i> / <i>ipv6</i> ]   <i>ipip</i>   <i>ipipv6</i>   <i>ipv6ip6</i>   <i>ipv6ip</i> [ <i>6to4</i> / <i>isatap</i> ] }	Optional By default, the working mode of the Tunnel interface is GRE over IPv4
Configure TOS of the Tunnel interface	<b>tunnel tos</b> <i>tos-value</i>	Optional By default, the Tunnel interface is not configured with TOS
Configure TTL of the Tunnel interface	<b>tunnel ttl</b> <i>ttl-value</i>	Optional By default, the TTL value of the Tunnel interface is 255

---

### Note

- The TOS value configured on the Tunnel interface is used to fill in the TOS field in the header of the outer IPv4 packet during encapsulation. If the TOS value is not configured on the Tunnel interface, use the TOS value in the header of the inner IPv4 packet instead.
  - The TTL value configured on the Tunnel interface is used to fill in the TTL field in the header of the outer IPv4 packet during encapsulation.
- 

## 23.2.2 Tunnel Interface Monitoring and Maintaining

Table 23-3 Tunnel Interface Monitoring and Maintaining

Command	Description
<b>enable</b>	Privileged mode
<b>debug tunnel {all   config   event   forward   packet }</b>	Enable the Tunnel debugging information switch
<b>show tunnel [tunnel-id] [slot slot-num]</b>	Display tunnel information

# 24 VXLAN Interface

## 24.1 Overview

The VXLAN interface is one logical interface used for L3 forwarding between different VXLAN instances. One VXLAN instance can only be bound to one VXLAN interface, and also, one VXLAN interface can only be bound to one VXLAN instance. The numbers of the VXLAN instances correspond to the VXLAN interfaces one by one.

## 24.2 VXLAN Interface Function

Table 24-1 VXLAN Interface Function Configuration List

Configuration Task	
Configure functions of the VXLAN Interface	Configure basic functions of the VXLAN Interface
	Configure distributed gateway of the VXLAN interface

## 24.2.1 Configure basic functions of the VXLAN Interface

### Configuration Condition

None

### Configure basic functions of the VXLAN Interface

Table 24-2 Configuring Basic Functions of VXLAN Interface

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Create VXLAN interface	<b>interface vxlan vxlan-id</b>	Mandatory By default, no VXLAN interface is created

### Note

- VXLAN interface is one logical interface. To make sure it works normally, you need to create a VXLAN instance with a corresponding number, and the VXLAN instance needs to be associated with a VXLAN access port or VXLAN tunnel that is UP. For how to build a VXLAN network, refer to the relevant chapters in User Manual VXLAN.

## 24.2.2 Configure Distributed Gateway Function of VXLAN

Table 24-3 Configuring Distributed Gateway Function of VXLAN Interface

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter VXLAN interface mode	<b>interface vxlan vxlan-id</b>	-
Configure Distributed Gateway Function of VXLAN	<b>vxlan distribute-gateway</b>	Optional

Step	Command	Description
		Enable the distributed gateway function  By default, the distributed gateway of VXLAN is not enabled

### 24.2.3 VXLAN Interface Monitoring and Maintaining

Table 24-4 VXLAN Interface Monitoring And Maintaining

Command	Description
<b>show interface vxlan</b> <i>vxlan-id</i>	View the information of the specified VXLAN interface

# 25 Link Aggregation

---

## 25.1 Overview

Through link aggregation, multiple physical links between two devices are bound to form a logic link so as to expand link capacity. Within the logic link, the physical links act as redundancy and dynamic backup of each other, providing higher network connection reliability.

## 25.1.1 Basic Concepts

### Aggregation Group and Member Ports

Multiple physical ports are bound to form an aggregation group, and the physical ports are member ports of the aggregation group.

### Member Port Status

The member ports of an aggregation group have the following two statuses:

- **Selected:** The member ports which are in this status can participate in user service traffic forwarding. The member ports in this status are called "the selected ports".
- **Unselected:** The member ports which are in this status cannot participate in user service traffic forwarding. The member ports in this status are called "the unselected ports".

The rate and duplex mode of an aggregation group is determined by the selected ports in the aggregation group. The rate of an aggregation group is the sum of all selected ports, and the duplex mode of the aggregation group is the same as the duplex mode of the selected ports.

### Operation Key

An operation key is the property configuration of member ports. It consists of the rate, duplex mode, and administrative key (that is, the aggregation group number). In property configuration, change of the duplex mode or rate may cause re-calculation of the operation key.

In one aggregation group, if the duplex modes or rates of member ports are different, then the generated operation keys are different. However, the member ports that are in the selected status must have the same operation key.

### LACP

Link Aggregation Control Protocol (LACP) is a protocol that is based on IEEE802.3ad. In LACP, Link Aggregation Control Protocol Data Units (LACPDU) are used to interchange messages between two ends.

### LACP Priorities

LACP priorities are categorized into two types: system LACP priorities and port LACP priorities.

- **System LACP priorities:** They are used to determine the LACP priority order of the devices at two ends.
- **Port LACP priorities:** They are used to determine the priority order at which the member ports of the local device are selected.

### System ID and Port ID

**System ID:** Aggregation property of a device. It consists of the system LACP priority of the device and the system MAC address. The higher the system LACP priority is, the better the system ID of the device is. If

the system LACP priorities are the same, then the smaller the system MAC address is, the better the system ID of the device is.

Port ID: Aggregation property of a port. It consists of the port LACP priority and the port number. The higher the port LACP priority is, the better the port ID is. If the port LACP priorities are the same, then the smaller the port number is, the better the port ID is.

### Root Port of an Aggregation Group

The protocols that are applied in an aggregation group receive and send protocol packets through the root port of the aggregation group. The root port of an aggregation group is selected from the member ports of the aggregation group. The physical link of the root port must be in the up status.

### 25.1.2 Link Aggregation Modes

Link aggregation modes include the static aggregation mode and the dynamic aggregation mode. Aggregation groups are categorized into static aggregation groups and dynamic aggregation groups.

#### Static Aggregation Mode

In static aggregation mode, the LACP protocol of the member ports of the devices at the two ends is in the disabled status. In the static aggregation group of the local device, set the selected and unselected status for the member ports by following the guidelines as described below:

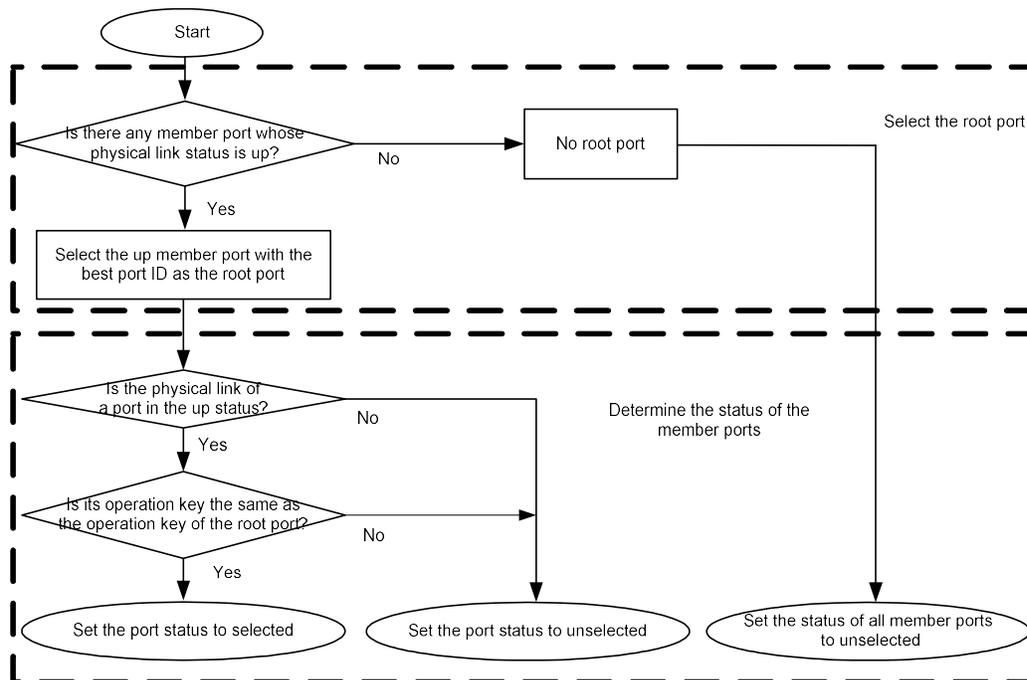


Figure 25 Setting the Status of Member Ports in Static Aggregation Mode

#### Dynamic Aggregation Mode

In dynamic aggregation ports, a port can join in a dynamic aggregation group in two modes, active or passive.

- If the duplex mode of the port is full duplex:

If the port joins in a dynamic aggregation group in active mode, the LACP protocol is enabled for the port.

If the port joins in a dynamic aggregation group in passive mode, the LACP protocol is disabled for the port. After it receives the LACPDU packets from the peer port, the LACP protocol is enabled.

- If the duplex mode of the port is half duplex, no matter the port joins in a dynamic aggregation group in either mode, the LACP protocol is disabled for the port.

In the dynamic aggregation group, set the selected and unselected status for the member ports by following the guidelines as described below:

First determine the device with a better system ID. Then the device determines the statuses of the member ports of the devices at the two ends. The device with the better system ID sets the selected and unselected status for the member ports by following the guidelines as described below:

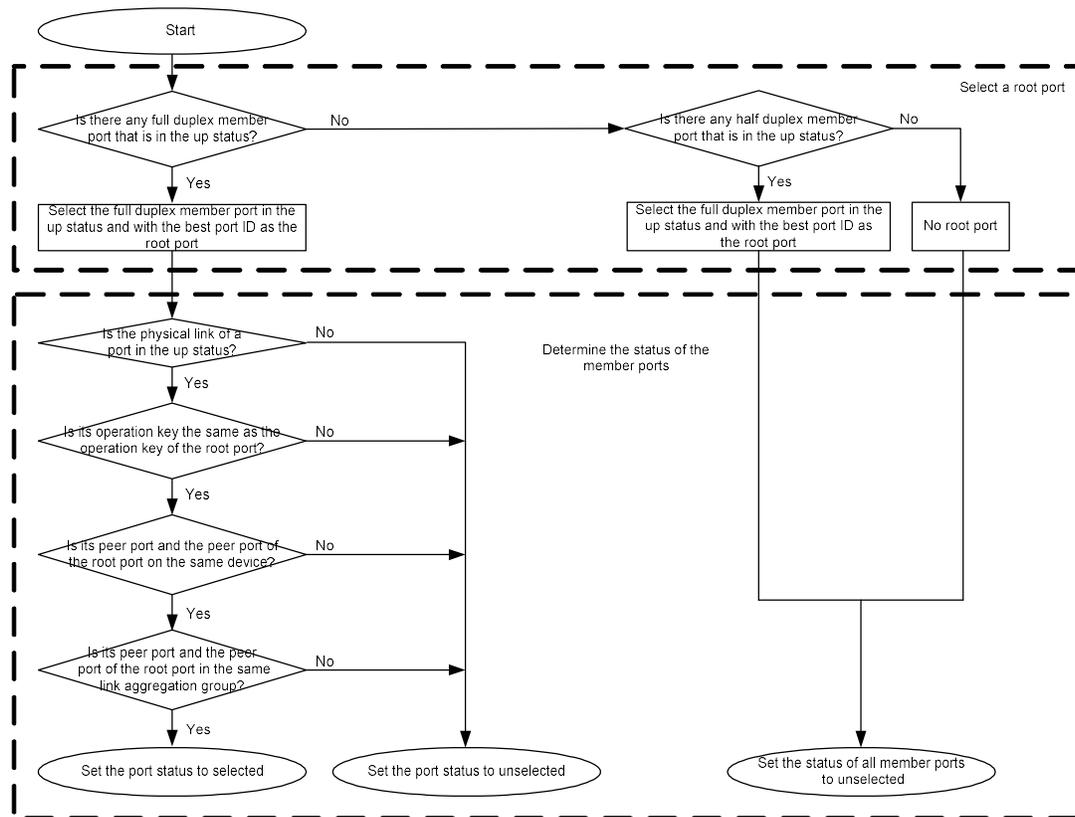


Figure 1 Setting the Status of Member Ports in Dynamic Aggregation Mode

## 25.2 Overview

### 25.2.1 Load balancing

Load balance means when the traffic outlet is an aggregation group/ECMP group, chips can enable traffic to realize load balancing between member ports within the aggregation group/ECMP group according to current HASH configuration conditions to improve the bandwidth availability ratio of aggregation group/ECMP group.

### 25.2.2 HASH KEY

HASH KEY means the KEY value calculated by chips through HASH for port when the traffic selects the specific port of aggregation group/ECMP group. Generally, different packet types and different switching chips support different values of HSAH KEY. The HASH KEYs supported by different packets are shown in Table 1-1.

Table 25 Values of HASH KEY Supported by Different Types of Packet and Their Meanings

Type of HASH KEY	Description
dst-mac	Based on destination MAC address: Realize aggregation load balancing by the destination MAC address of packet.
src-mac	Based on source MAC address: Realize aggregation load balancing by the source MAC address of packet.
src-interface	Based on receiving source interface: Realize aggregation load balancing by the receiving source interface of packet.
vlan	Based on VLAN: Realize aggregation load balancing by the VLAN of packet.
dst-ip	Based on destination IP address: Realize aggregation load balancing by the destination IP address of packet.
l4-dst-port	Based on layer-4 destination port number: Realize aggregation load balancing by the four-layer destination port number of packet.

Type of HASH KEY	Description
protocol	Based on IP protocol: Realize aggregation load balancing by the IP protocol of packet.
src-ip	Based on source IP address: Realize aggregation load balancing by the source IP address of packet.
l4-src-port	Based on layer-4 source port number: Realize aggregation load balancing by the layer-4 source port number of packet.
Top-label	Realize load balancing based on mpls packet header
2nd-label	Realize load balancing based on layer-2 tag of mpls packet
ingress-nickname	Realize aggregation load balancing by the ingress nickname of packet
egress-nickname	Realize aggregation load balancing by the egress nickname of packet

For this device, the HASH KEYS supported by different packets are shown in Table 1-2:

Table 1 HASH KEYS Supported by Different Packets

Type of Packet	HASH KEY Support
Known unicast packet in L2	dst-mac, src-mac, src-interface, vlan
Known unicast packet in L3 (IPv4/IPv6)	dst-ip, l4-dst-port, protocol, src-ip, l4-src-port, src-interface
Other packets in L2	dst-mac, src-mac, src-interface
Other packets in L3 (IPv4/IPv6)	dst-ip, src-ip, src-interface
Mpls packet	Src-ip, dst-ip, top-label, 2nd-label
Vxlan packet	dst-mac, src-mac, vlan, dst-ip, src-ip, protocol, l4-src-port, l4-dst-port

Type of Packet	HASH KEY Support
Trill packet	dst-mac、 src-mac、 vlan、 egress-nickname、 ingress-nickname

---

### Note

- The HASH KEY of known unicast packet in L2 can support a combination of one or more combination HASH KEYs.
  - The HASH KEY of known unicast packet in L3 (IPV4/IPV6) can support a combination of one or more combination HASH KEYs. The HASH KEYs of other L2 packets are fixed and cannot be configured. They use dst-mac, src-mac, and src-interface for load balancing.
  - The HASH KEYs of other L3 (IPv4/IPv6) packets are fixed and cannot be configured. They use dst-ip, src-ip and src-interface for load balancing.
- 

### 25.2.3 Load balancing mode

Load balancing mode is a "user-mode" concept specially introduced to shield the difference of chips from different chip manufacturers. In particular, "user" means to all the services that need to use chip load balancing (i.e., business modules, such as aggregation LAC); "mode" is a reusable HASH configuration plan that abstracts underlying HASH resource.

Load balancing mode is distinguished by mode name which has less than 31 characters. By default, there is a default HASH mode "default" in the system. Besides, there are 6 modes that complete load balancing based on mode name. They can be referenced, but cannot be configured. The "default" mode generally comprises the HASH KEY configuration of L2 packets/L3 packets/MPLS packets/VXLAN packets/TRILL packets. Users may flexibly configure the load balancing mode and the HASH KEY of corresponding mode as needed. Upon completion of the configuration, they can realize load balancing of traffic according to corresponding mode configuration by referring or binding corresponding mode.

---

### Note

- The default load balancing mode name "default" cannot be modified.
  - The default load balancing mode "default" cannot be deleted, but can be configured.
- 

## 25.3 Function configuration of load balancing mode

Table 2 Function Configuration List of Load Balancing Mode

Configuration Task	
Load balancing mode configuration function	Enter the mode configuration mode
	Configure the HASH KEY of load balancing mode
	Configure the load selection of ip tunnel packet
	Configure the load selection of mpls, vxlan and trill packet
	Configure the algorithm selection of LAC load
	Configure the algorithm selection of ECMP load
	Configure the algorithm selection of ipv6 packet address
	Configure the deep analysis algorithm for ip, mpls, and vxlan packet of load balancing mode

### 25.3.1 Enter the load balancing mode

After successfully entering the load balancing mode, you may configure its mode.

#### Note

- Users can create 0 custom mode at most.

#### Configuration Condition

None

#### Create load balancing mode

Table 1-4 Entering Load Balancing Mode

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the load balancing mode	<b>load-balance profile default</b>	Mandatory

---

## Note

- By default, the "default" mode has been created by the system. Users can directly enter the configuration mode of the "default" mode through the creation command.
  -
- 

### 25.3.2 Configure the HASH KEY of load balancing mode

After successfully entering the mode configuration mode, you can configure the HASH KEY value of corresponding load balancing mode.

---

## Note

- The "default" mode created by the system by default will configure a set of default HASH KEY. Users can modify the configuration as needed.
  - The default configurations of the "default" mode are as follows: L2: src-mac, dst-mac; Ipv4/Ipv6: src-ip, dst-ip, l4-src-port, l4-dst-port; mpls: src-ip, dst -ip; vxlan: src-mac, dst-mac, l4-src-port, l4-dst-port; trill: src-mac, dst-mac.
- 

---

## Caution

- The configuration of HASHKEY can become effective only after it is activated by executing active configuration pending.
- 

### Configuration Condition

None

### Configure the HASH KEY of load balancing mode

Table 3 HASH KEY Configuration of Load Balancing Mode

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the load balancing mode configuration mode	<b>load-balance profile</b> default	Mandatory Enter the configuration mode of default mode

Step	Command	Description
Configure the HASH KEY used by L2 known unicast packet load	<b>l2</b> { [ <b>dst-mac</b> ] [ <b>src-mac</b> ] [ <b>src-interface</b> ] [ <b>vlan</b> ] }	Mandatory One or more HASH KEYs can be combined
Configure the HASH KEY used by known unicast packet in L3 (IPV4/IPV6)	<b>Ipv4/Ipv6</b> { [ <b>dst-ip</b> ] [ <b>I4-src-port</b> ] [ <b>I4-dst-port</b> ] [ <b>protocol</b> ] [ <b>src-interface</b> ] [ <b>src-ip</b> ] }	Mandatory One or more HASH KEYs can be combined
Configure the HASH KEY used by mpls packet load	<b>Mpls</b> {[ <b>src-ip</b> ] [ <b>dst-ip</b> ] [ <b>top-label</b> ] [ <b>2nd -lable</b> ] }	Mandatory One or more HASH KEYs can be combined
Configure the HASH KEY used by vxlan packet load	<b>Vxlan</b> {[ <b>src-mac</b> ][ <b>dst-mac</b> ][ <b>vlan</b> ] [ <b>src-ip</b> ][ <b>dst-ip</b> ][ <b>protocol</b> ] [ <b>I4-src-port</b> ][ <b>I4-dst-port</b> ]}	Mandatory One or more HASH KEYs can be combined
Configure the HASH KEY used by trill packet load	<b>Trill</b> {[ <b>src-mac</b> ][ <b>dst-mac</b> ][ <b>vlan</b> ] [ <b>sgress-nickname</b> ][ <b>ingress-nickname</b> ]}	Mandatory One or more HASH KEYs can be combined
Activate current HASH KEY configuration	<b>active configuration pending</b>	Mandatory
Cancel current HASH KEY configuration	<b>abort configuration pending</b>	Mandatory

## Note

- Configure HASH KEY value through l2/IPV4/IPV6/MPLS/VXLAN/TRILL command. It cannot not take effect immediately when in pending status. Only active configuration pending can make it effective.
- Configure HASH KEY value through l2/IPV4/IPV6/MPLS/VXLAN/TRILL command. It cannot not take effect immediately when in pending status. Users may cancel the current configuration by using the abort configuration pending command.
- When a new HASH KEY is configured, the original HASH KEY will not be overwritten. The result of activation with the active command combines both the

original HASH KEY and the new one.

- When the HASH KEY in pending status is canceled with the abort command, the original HASH KEY will not be modified.
- When the activation fails, which is generally because the HASH KEY configured doesn't meet the requirements, the pending HASH KEY will not be cleared.
- Requirements for "default" mode: The HASH KEYs of L2 and IPV4/IPV6 shouldn't be empty at the same time, and corresponding HASHKEY shouldn't be empty either when the MPLS/VXLAN/TRILL service is bound to the mode.

### 25.3.3 Configure the deep analysis algorithm for ipv4/ipv6 packet of load balancing mode

After entering the mode configuration mode, you can configure the deep analysis algorithm of corresponding load balancing mode for ipv4/ipv6 packet.

#### Configuration Condition

Under mode configuration mode

#### Configure the deep analysis algorithm for ipv4/ipv6 packet of load balancing mode

Table 4 Configuring Deep Analysis Algorithm for ipv4/ipv6 Packet of Load Balancing Mode

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the load balancing mode configuration mode	<b>load-balance profile default</b>	Mandatory Enter the configuration mode of default mode
Configure the deep analysis algorithm for ipv4/ipv6 packet	<b>hash-control depth-parse ipv4/ipv6</b> { [enable][disable] }	enable: ip packet hash based on ip header disable: ip packet hash based on mac

### 25.3.4 Configure the deep analysis algorithm for mpls and vxlan packet of load balancing mode

After entering the mode configuration mode, you can configure the deep analysis algorithm of corresponding load balancing mode for mpls and vxlan packet.

#### Configuration Condition

Under mode configuration mode

## Configure the deep analysis algorithm for mpls and vxlan packet of load balancing mode

Table 5 Configuring Deep Analysis Algorithm for mpls and vxlan Packet of Load Balancing Mode

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the load balancing mode configuration mode	<b>load-balance profile default</b>	Mandatory Enter the configuration mode of default mode
Configure the deep analysis algorithm for mpls packet	<b>hash-control depth-parse mpls { [enable][disable] }</b>	enable: load balancing for packet based on mpls header  diabile: load balancing for packet based on layer-3 or layer-2 header
Configure the deep analysis algorithm for vxlan packet	<b>hash-control depth-parse vxlan{ [enable][disable] }</b>	enable: load balancing for packet based on vxlan header  diabile: load balancing for packet based on layer-3 or layer-2 header

### 25.3.5 Configure the load selection for ip tunnel packet of load balancing mode

After entering the mode configuration mode, you can configure the load selection of corresponding load balancing mode for ip tunnel packet.

#### Configuration Condition

Under mode configuration mode

#### Configure the load selection for ip tunnel packet of load balancing mode

Table 6 Configuring Load Selection for ip Tunnel Packet of Load Balancing Mode

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Enter the load balancing mode configuration mode	<b>load-balance profile</b> default	Mandatory Enter the configuration mode of default mode
Configure the deep analysis algorithm for v4inv4 packet	<b>hash-control depth-parse v4inv4</b> { [inner-header][ outer-header] }	inner-header: load selection for packet based on the inner layer header of v4inv4  outer-header: load selection for packet based on the outer layer header of v4inv4
Configure the deep analysis algorithm for v4inv6 packet	<b>hash-control depth-parse v4inv6</b> { [inner-header][ outer-header] }	inner-header: load selection for packet based on the inner layer header of v4inv6  outer-header: load selection for packet based on the outer layer header of v4inv6
Configure the deep analysis algorithm for v6inv4 packet	<b>hash-control depth-parse v6inv4</b> { [inner-header][ outer-header] }	inner-header: load selection for packet based on the inner layer header of v6inv4  outer-header: load selection for packet based on the outer layer header of v6inv6
Configure the deep analysis algorithm for v6inv6 packet	<b>hash-control depth-parse v6inv6</b> { [inner-header][ outer-header] }	inner-header: load selection for packet based on the inner layer header of v6inv6  outer-header: load selection for packet

Step	Command	Description
		based on the outer layer header of v6inv6
Configure the deep analysis algorithm for v4grev4 packet	<b>hash-control depth-parse</b> v4grev4{ [inner-header][ outer-header] }	inner-header: load selection for packet based on the inner layer header of v4grev4  outer-header: load selection for packet based on the outer layer header of v4grev4
Configure the deep analysis algorithm for v4grev6 packet	<b>hash-control depth-parse</b> v4grev6{ [inner-header][ outer-header] }	inner-header: load selection for packet based on the inner layer header of v4grev6  outer-header: load selection for packet based on the outer layer header of v4grev6
Configure the deep analysis algorithm for v6grev4 packet	<b>hash-control depth-parse</b> v6grev4{ [inner-header][ outer-header] }	inner-header: load selection for packet based on the inner layer header of v6grev4  outer-header: load selection for packet based on the outer layer header of v6grev4

Step	Command	Description
Configure the deep analysis algorithm for v6grev6 packet	<b>hash-control depth-parse</b> v6grev6{ [inner-header][ outer-header] }	inner-header: load selection for packet based on the inner layer header of v6grev6  outer-header: load selection for packet based on the outer layer header of v6grev6

### 25.3.6 Configure the load selection for mpls, vxlan and trill packet of load balancing mode

After entering the mode configuration mode, you can configure the load selection of corresponding load balancing mode for mpls, vxlan and trill packet.

#### Configuration Condition

Under mode configuration mode

#### Configure the load selection for mpls, vxlan and trill packet of load balancing mode

Table 7 Configuring Load Selection for mpls, vxlan and trill Packet of Load Balancing Mode

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the load balancing mode configuration mode	<b>load-balance profile</b> default	Mandatory Enter the configuration mode of default mode
Configure the load selection for mpls packet	<b>hash-control mpls field</b> { [inner-l2][inner-l3] }	Inner-l2: load balancing for packet based on inner layer 2 of mpls  Inner-l3: load balancing for packet based on inner layer 3 of mpls

Step	Command	Description
Configure the load selection for vxlan packet	<b>hash-control vxlan field</b> { [inner-l2][inner-l3] }	Inner-l2: load balancing for packet based on inner layer 2 of vxlan  Inner-l3: load balancing for packet based on inner layer 3 of vxlan
Configure the load selection for trill packet	<b>hash-control trill field</b> { [inner-l2][inner-l3] }	Inner-l2: load balancing for packet based on inner layer 2 of trill  Inner-l3: load balancing for packet based on inner layer 3 of trill

### 25.3.7 Configure HASH algorithm selection for LAC and ECMP of load balancing mode

After entering the mode configuration mode, you can configure HASH algorithm selection for LAC and ECMP.

#### Configuration Condition

Under mode configuration mode

#### Configure HASH algorithm selection for LAC and ECMP of load balancing mode

Table 8 Configuring HASH Algorithm Selection for LAC and ECMP of Load Balancing Mode

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the load balancing mode configuration mode	<b>load-balance profile</b> default	Mandatory Enter the configuration mode of default mode
Configure algorithm selection for LAC	<b>hash-control algorithm</b> { XOR16   CRC32-LO   CRC32-HI   CRC16-CCITT	Configure the hash algorithm used when the egress is link aggregation

Step	Command	Description
	<pre> CRC16-BISYNC  CRC16-BISYNC-XOR1  CRC16- BISYNC-XOR2  CRC16-BISYNC- XOR4  CRC16-BISYNC-XOR8 }</pre>	
Configure algorithm selection for ECMP	<pre><b>hash-control algorithm</b> {XOR16  CRC32-LO  CRC32-HI  CRC16-CCITT  CRC16-BISYNC  CRC16-BISYNC-XOR1  CRC16- BISYNC-XOR2  CRC16-BISYNC- XOR4  CRC16-BISYNC-XOR8 }</pre>	Configure the hash algorithm used when the egress is ECMP

### 25.3.8 Configure algorithm selection for ipv6 address compression of load balancing mode

After entering the mode configuration mode, you can configure algorithm selection for ipv6 address compression of corresponding load balancing mode.

#### Configuration Condition

Under mode configuration mode

#### Configure algorithm selection for ipv6 address compression of load balancing mode

Table 9 Configuring Algorithm Selection for ipv6 Address Compression of Load Balancing Mode

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the load balancing mode configuration mode	<b>load-balance profile default</b>	Mandatory Enter the configuration mode of default mode

Step	Command	Description
Configure algorithm selection for ipv6 address compression	<b>hash-control ipv6 collapse</b> { [XOR][LSB] }	Select XOR algorithm by default

## 25.4 Link Aggregation Function Configuration

Table 10 Function Configuration List of Link Aggregation

Configuration Task	
Configure an Aggregation Group	Create an Aggregation Group
	Add Ports into the Aggregation Group
Configure LACP Priorities	Configure the System LACP Priority
	Configure the Port LACP Priority
Configure hot plug for rapid switch of root port	Configure hot plug for rapid switch of root port

### 25.4.1 Configure an Aggregation Group

Configuring the aggregation group can realize centralized management of multiple physical ports. Any configuration of the aggregation group will have an impact on all member ports.

#### Note

- Each aggregation group can support up to 16 ports at the same time.

#### Configuration Condition

None

#### Create an Aggregation Group

The aggregation groups at the two ends of an aggregated link must be configured to the same type. Description can be added to each aggregation group to make it easier for network administrators to distinguish the aggregation groups.

Table 11 Configuring Creation of Aggregation Group

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Create an Aggregation Group	<b>link-aggregation link-aggregation-id mode { manual   lacp }</b>	Mandatory By default, the aggregation group is not created.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation link-aggregation-id</b>	-
Configure aggregation group description information	<b>description description-name</b>	Optional By default, there is no aggregation group description information.
Configure description information for peer port of aggregation group	<b>peer-description description-name</b>	Optional By default, the aggregation group has no peer port description information.

## Caution

- The protocols that are applied in an aggregation group receive and send protocol packets through the root port of the aggregation group. In static aggregation mode, because the member ports between the devices at two ends do not exchange LACPDU packets, the root ports of the two devices may be on different physical links. In this way, other protocol packets on the aggregation group may fail to be received or sent. To prevent this problem, ensure that the root ports of the devices at the two ends are on the same physical link. In dynamic aggregation mode, the member ports of the devices at two ends exchange LACPDU packets. The negotiation between the two member ports ensures that the root ports of the two devices are on the same physical link.
- After an aggregation group is deleted, all the member ports of the aggregation group are removed from the aggregation group, and then all the member ports adopt the default settings. This may result in loops in the network. Therefore, before deleting an aggregation group, ensure that the spanning tree function has been enabled or ensure that no loop may occur in the network.

## Add Ports into the Aggregation Group

When an aggregation group is created, it is only a logic interface which contains no physical port. In this case, the aggregation function does not take effect. The aggregation function takes effect after ports are added to a static aggregation group. The aggregation function takes effect after local or peer ports are added into a dynamic aggregation group.

Table 12 Addition of Ports into Aggregation Group

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	-
Add Ports into the Aggregation Group	<b>link-aggregation</b> <i>link-aggregation-id</i> { <b>manual</b>   <b>active</b>   <b>passive</b> }	Mandatory By default, the port is not added into any aggregation group.

---

### Note

- Before adding a port into an aggregation group, the aggregation group must have been created; otherwise, an error message is displayed.
  - A port can be added one aggregation group at a time.
  - After a port is added into an aggregation group, the some existing configurations (such as loopback detection and VLAN) will be removed from the port.
  - Some functions (such as loopback detection) cannot be configured on a member port in an aggregation group; otherwise, an error message is displayed.
  - If a port is added into a dynamic aggregation group in passive mode, its peer port must be added into the dynamic aggregation group in active mode. Otherwise, the two ports are both in the unselected status and they cannot participate in user service traffic forwarding.
- 

## 25.4.2 Configure LACP Priorities

### Configuration Condition

None

### Configure the System LACP Priority

Configuration of the system LACP priority may affect the system ID, and finally affect the selected/unselected status of member ports of dynamic aggregation groups.

Table 13 Configuration of System LACP Priority

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the System LACP Priority	<b>lacp system-priority</b> <i>system-priority-value</i>	Mandatory By default, the system LACP priority is 32768.

### Configure the Port LACP Priority

Configuration of the port LACP priority may affect the port ID, and finally affect the selected/unselected status of member ports of aggregation groups.

Table 1-16 Configuration of Port LACP Priority

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	-
Configure the Port LACP Priority	<b>lacp port-priority</b> <i>port-priority-value</i>	Mandatory By default, the port LACP priority is 32768.

### 25.4.3 Configure hot plug for rapid switch of root port

Configure a hot plug for rapid switch of root port so that when the board where the root port is located is hot-plugged, the peer port can be quickly notified to reselect a root port for rapid stabilization and convergence of the aggregation group.

---

 **Note**

- The rapid switch notice will be sent only when the board where the root port is located is pulled out.
  - Static aggregation group will not send rapid switch notice.
- 

**Configuration Condition**

None

**Configure hot plug for rapid switch of root port**

Table 14 Configuration of Hot Plug for Rapid Switch of Root Port

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure hot plug for rapid switch of root port	<b>link-aggregation hotswap fast-change-rootport</b>	Mandatory By default, hot plug for rapid switch of root port is not configured.

## 25.4.4 Link Aggregation Monitoring and Maintaining

Table 15 Link Aggregation Monitoring and Maintaining

Command	Description
<b>show link-aggregation group</b> [ <i>link-aggregation-id</i> ]	Displays brief information about a specified aggregation group or all existing aggregation groups.
<b>show link-aggregation interface</b> [ <i>interface-name</i> ]	Displays the details of a specified member port of an aggregation group or details of all member ports of the aggregation group.

## 25.5 Typical Configuration Example of Link Aggregation

### 25.5.1 Configure a Static Aggregation Group

#### Network Requirements

- Device1 is connected to PC1, Device2 is connected to PC2 and PC3, and the three PCs are in the same network segment. Device1 and Device2 are interconnected through Trunk ports.
- A static aggregation group is configured between Device1 and Device2 for bandwidth increase, load sharing, and service backup.

#### Network Topology

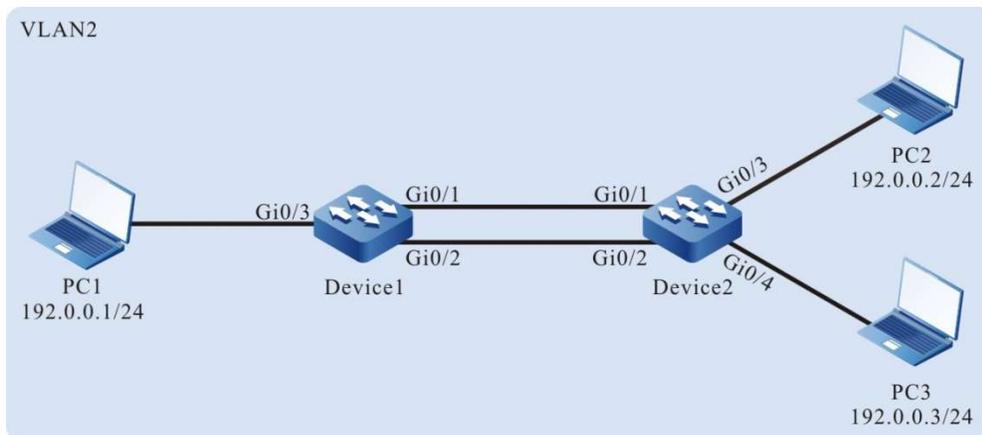


Figure 2 Networking for Configuring a Static Aggregation Group

#### Configuration Steps

*Step 1:* Create a static aggregation group.

#On Device1, create static aggregation group 1.

```
Device1#configure terminal
Device1(config)#link-aggregation 1 mode manual
```

#On Device2, create static aggregation group 2.

```
Device2#configure terminal
Device2(config)#link-aggregation 1 mode manual
```

*Step 2:* Add ports into the aggregation group.

#On Device1, add ports gigabitethernet0/1 and gigabitethernet0/2 into aggregation group 1 in Manual mode.

```
Device1(config)#interface gigabitethernet 0/1,0/2
Device1(config-if-range)#link-aggregation 1 manual
Device1(config-if-range)#exit
```

#On Device2, add ports gigabitethernet0/1 and gigabitethernet0/2 into aggregation group 1 in Manual mode.

```
Device2(config)#interface gigabitethernet 0/1,0/2
Device2(config-if-range)#link-aggregation 1 manual
Device2(config-if-range)#exit
```

#After the configuration is completed, check the status of aggregation group 1 on the devices.

Here takes Device1 for example:

```
Device1#show link-aggregation group 1
Link Aggregation 1
Type: switchport
Mode: Manual
User: LAC
Description:
Peer-description:
Least active-linknumber: 1
Maximal active-linknumber: 16
Load balance profile: default
Number of ports in total: 2
Number of ports attached: 2
Root port: gigabitethernet0/1
gigabitethernet0/1: ATTACHED
gigabitethernet0/2: ATTACHED
```

According to the system display, ports gigabitethernet0/1 and gigabitethernet0/2 are both in the ATTACHED state in aggregation group 1, and aggregation of aggregation group 1 is successful.

---

## Note

- For the method of checking Device2, refer to the method of checking Device1.
- 

*Step*  
3:

Configure the load balancing mode of the aggregation group.

# Enter default of load balancing mode on Device1.

```
Device1(config)#load-balance profile default
```

# Under the default of load balancing mode on Device1, configure the packet load hash-key, make L2 packet loaded by destination MAC, and make IP packet loaded by destination IP.

```
Device1(config-userProfile-default)#l2 dst-mac
Device1(config-userProfile-default)#ip dst-ip
Device1(config-userProfile-default)#active configuration pending
```

*Step* 4: Configure a VLAN, and configure the link type of the aggregation group and ports.

#On Device1, create VLAN2, configure the link type of aggregation group 1 as Trunk, allow services of VLAN2 to pass, and configure PVID as 2.

```
Device1(config)#vlan 2
Device1(config-vlan2)#exit
Device1(config)#interface link-aggregation 1
Device1(config-link-aggregation1)#switchport mode trunk
Device1(config-link-aggregation1)#switchport trunk allowed vlan add 2
Device1(config-link-aggregation1)#switchport trunk pvid vlan 2
Device1(config-link-aggregation1)#exit
```

#On Device1, configure the link type of port gigabitethernet0/3 as Access, and allow services of VLAN2 to pass.

```
Device1(config)#interface gigabitethernet 0/3
Device1(config-if-gigabitethernet0/3)#switchport mode access
Device1(config-if-gigabitethernet0/3)#switchport access vlan 2
Device1(config-if-gigabitethernet0/3)#exit
```

#On Device2, create VLAN2, configure the link type of aggregation group 1 as Trunk, allow services of VLAN2 to pass, and configure PVID as 2. (Omitted)

#On Device2, configure the link type of ports gigabitethernet0/3 and gigabitethernet0/4 as Access, and allow services of VLAN2 to pass. (Omitted)

*Step* 5: Check the result.

#Check the aggregation bandwidth of aggregation group 1 on the devices.

Here takes Device1 for example:

```
Device1#show interface link-aggregation 1
link-aggregation 1 configuration information
  Description      :
  Peer-description :
  Status           : Enabled
  Link             : Up
  Act Speed        : 2000
  Act Duplex       : Full
  Port Type        : Nni
  Pvid             : 2
```

According to the system display, the interface bandwidth of the aggregation group 1 on Device1 is 2000 M.



- 
- For the method of checking Device2, refer to the method of checking Device1.
- 

#During the process of service interaction between PC1 and PC2 and PC3, load balancing of data is achieved on the aggregated links. If a link in the aggregation group becomes faulty, the other links provide service backup.

## 25.5.2 Configure a Dynamic Aggregation Group

### Network Requirements

- Device1 is connected to PC1, Device2 is connected to PC2 and PC3, and the three PCs are in the same network segment. Device1 and Device2 are interconnected through Trunk ports.
- A dynamic aggregation group is configured between Device1 and Device2 for bandwidth increase, load sharing, and service backup.

### Network Topology

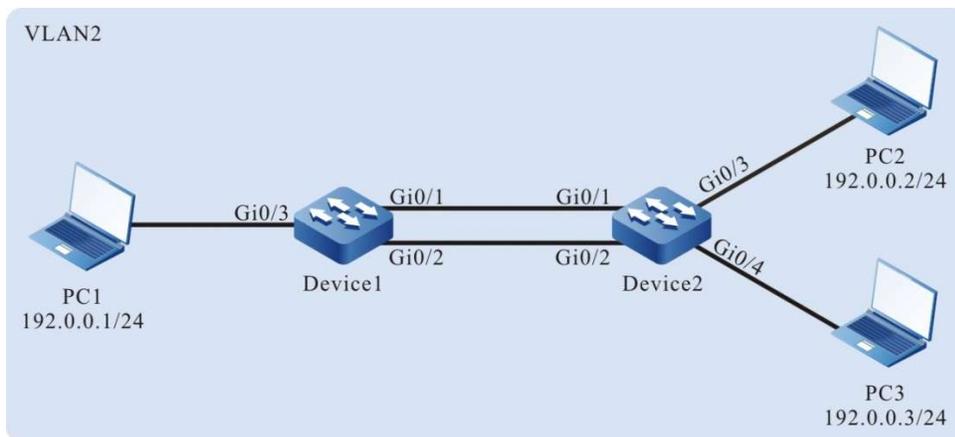


Figure 3 Networking for Configuring a Dynamic Aggregation Group

### Configuration Steps

*Step 1:* Create a dynamic aggregation group.

#On Device1, create dynamic aggregation group 1.

```
Device1#configure terminal
Device1(config)#link-aggregation 1 mode lacp
```

#On Device2, create dynamic aggregation group 1.

```
Device2#configure terminal
Device2(config)#link-aggregation 1 mode lacp
```

*Step*  
2: Add ports into the aggregation group.

#On Device1, add ports gigabitethernet0/1 and gigabitethernet0/2 into aggregation group 1 in Active mode.

```
Device1(config)#interface gigabitethernet 0/1,0/2
Device1(config-if-range)#link-aggregation 1 active
Device1(config-if-range)#exit
```

#On Device2, add ports gigabitethernet0/1 and gigabitethernet0/2 into aggregation group 1 in Active mode.

```
Device2(config)#interface gigabitethernet 0/1,0/2
Device2(config-if-range)#link-aggregation 1 active
Device2(config-if-range)#exit
```

#After the configuration is completed, check the status of aggregation group 1 on the devices.

Here takes Device1 for example:

```
Device1#show link-aggregation group 1
Link Aggregation 1
Type: switchport
Mode: LACP
User: LAC
Description:
Peer-description:
Least active-linknumber: 1
Maximal active-linknumber: 16
Load balance profile: default
Number of ports in total: 2
Number of ports attached: 2
Root port: gigabitethernet0/1
gigabitethernet0/1: ATTACHED
gigabitethernet0/2: ATTACHED
```

According to the system display, ports gigabitethernet0/1 and gigabitethernet0/2 are both in the ATTACHED state in aggregation group 1, and aggregation of aggregation group 1 is successful.

---

### Note

- For the method of checking Device2, refer to the method of checking Device1.
- 

*Step*  
3: Configure the load balancing mode of the aggregation group.

# Enter default of load balancing mode on Device1.

```
Device1(config)#load-balance profile default
```

# Under the default of load balancing mode on Device1, configure the packet load hash-key, make L2 packet loaded by destination MAC, and make IP packet loaded by destination IP.

```
Device1(config-userProfile-default)#l2 dst-mac
Device1(config-userProfile-default)#ip dst-ip
```

Device1(config-userProfile-default)#active configuration pending

*Step*  
4: Configure a VLAN, and configure the link type of the aggregation group and ports.

#On Device1, create VLAN2, configure the link type of aggregation group 1 as Trunk, allow services of VLAN2 to pass, and configure PVID as 2.

```
Device1(config)#vlan 2
Device1(config-vlan2)#exit
Device1(config)#interface link-aggregation 1
Device1(config-link-aggregation1)#switchport mode trunk
Device1(config-link-aggregation1)#switchport trunk allowed vlan add 2
Device1(config-link-aggregation1)#switchport trunk pvid vlan 2
Device1(config-link-aggregation1)#exit
```

#On Device1, configure the link type of port gigabitethernet0/3 as Access, and allow services of VLAN2 to pass.

```
Device1(config)#interface gigabitethernet 0/3
Device1(config-if-gigabitethernet0/3)#switchport mode access
Device1(config-if-gigabitethernet0/3)#switchport access vlan 2
Device1(config-if-gigabitethernet0/3)#exit
```

#On Device2, create VLAN2, configure the link type of aggregation group 1 as Trunk, allow services of VLAN2 to pass, and configure PVID as 2. (Omitted)

#On Device2, configure the link type of ports gigabitethernet0/3 and gigabitethernet0/4 as Access, and allow services of VLAN2 to pass. (Omitted)

*Step*  
5: Check the result.

#Check the aggregation bandwidth of aggregation group 1 on the devices.

Here takes Device1 for example:

```
Device1#show interface link-aggregation 1
link-aggregation 1 configuration information
  Description      :
  Peer-description :
  Status           : Enabled
  Link             : Up
  Act Speed        : 2000
  Act Duplex       : Full
  Port Type        : Nni
  Pvid             : 2
```

According to the system display, the interface bandwidth of the aggregation group on Device1 is 2000 M.

---

 **Note**

- For the method of checking Device2, refer to the method of checking Device1.
- 

#During the process of service interaction between PC1 and PC2 and PC3, load balancing of data is achieved on the aggregated links. If a link in the aggregation group becomes faulty, the other links provide service backup.

# 26 Port Isolation

---

## 26.1 Overview

Port isolation is a security feature that is based on ports. According to the actual requirement, you can configure certain ports to be isolated from a specified port, that is, configure some isolated ports for a specified port. In this way, the packets that are received by the specified port cannot be forwarded to the isolated ports. This enhances the network security, and also provides a flexible networking scheme.

## 26.2 Port Isolation Function Configuration

Table 26 Function Configuration List of Port Isolation

Configuration Task	
Configure the basic function of port isolation.	Configure port isolation.
Configure the isolation function for member ports of the aggregation group.	Configure isolation function for member ports of the aggregation group.

### 26.2.1 Configure the basic function of port isolation.

The port isolation function realizes unidirectional packet isolation. Assuming that port B is configured as the isolated port of port A, then if a packet whose target port is port B enters port A, the port is directly discarded. However, if a packet whose target port is port B enters port B, the port is normally forwarded. The isolated port can be a port or an aggregation group.

Port isolation, configured based on aggregation group.

- Ports in the same isolation group are isolated from each other.
- Ports in the isolation group can be configured as ingress, egress and both. The analysis

is shown below:

Table 26 Configure Mode Forwarding

Packet ingress port mode	Packet egress port mode	Whether it can be normally forwarded
ingress mode	ingress mode	Normal forwarding
ingress mode	egress mode	Locked
ingress mode	both mode	Locked
egress mode	ingress mode	Normal forwarding
egress mode	egress mode	Normal forwarding
egress mode	both mode	Normal forwarding
both mode	ingress mode	Normal forwarding
both mode	egress mode	Locked
both mode	both mode	Locked

- Ports in the isolation group normally communicate with those not in the isolation group
- Ports in different isolation groups can normally communicate with each other

### Configuration Condition

Isolation group has been created

### Configure port isolation.

Table 1 Configuration of Port Isolation

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter isolation group configuration mode	<b>isolate group <i>group-id</i></b>	Mandatory

Step	Command	Description
Add ports into the isolation group	<b>interface</b> <i>interface-list</i> [ <b>ingress</b>   <b>egress</b>   <b>both</b> ]	Mandatory  By default, the port is not added into any isolation group.
Add aggregation group into the isolation group.	<b>interface link-aggregation</b> <i>link-aggregation-id</i> [ <b>ingress</b>   <b>egress</b>   <b>both</b> ]	Mandatory  By default, the aggregation group is not added into any isolation group.

---

### Note

- When the port is added into an isolation group, the isolation group needs to be created.
- 

## 26.2.2 Port Isolation Monitoring and Maintaining

Table 26 Port Isolation Monitoring and Maintaining

Command	Description
<b>show isolate</b> { <b>group</b> [ <i>group-id</i> ]   <b>interface</b> <i>interface-list</i>   <b>interface link-aggregation</b> <i>link-aggregation-id</i> }	Show port isolation information

## 26.3 Typical Configuration Example of Port Isolation

### 26.3.1 Configure port isolation.

#### Network Requirements

- Connect PC1 and PC2 to Device, in the same VLAN2.
- Configure port isolation on Device so that PC1 and PC2 cannot communicate with each other.

## Network Topology

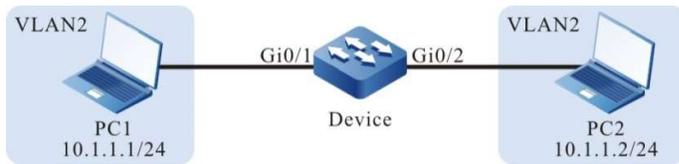


Figure 26 Configuration of Network Topology for Port Isolation

## Configuration Steps

*Step 1:* Configure VLANs and the link type of the ports.

# Create VLAN2 on Device.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the link type of ports gigabitethernet0/1 and gigabitethernet0/2 on Device as Access, allowing the services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/1-0/2
Device(config-if-range)#switchport mode access
Device(config-if-range)#switchport access vlan 2
Device(config-if-range)#exit
```

*Step 2:* Configure port isolation.

#Configure isolation group on Device

```
Device#config terminal
Device(config)#isolate group 1
Device(config-isolate-group 1)#
Device(config-isolate-group 1)#end
Device#show isolate group 1
-----
        isolate group 1
ingress member:
egress member :
both member  :
```

#Configure mutual isolation for ports gigabitethernet0/1 and gigabitethernet0/2 on Device.

```
Device#config terminal
Device(config)#isolate group 1
Device(config-isolate-group 1)#interface gigabitethernet 0/1-0/2

Device#show isolate group 1
-----
        isolate group 1
ingress member:
egress member :
both members  : gi0/1-0/2
```

#View the information of port isolation on Device.

```
Device#show isolate interface gigabitethernet 0/1-0/2
interface gigabitethernet0/1 isolated information
isolate group 1 mode: both
isolated interface:
    gi0/2
interface gigabitethernet0/2 isolated information
isolate group 1 mode: both
isolated interface:
    gi0/1
```

*Step 3:* Check the result.

#PC1 cannot communicate with PC2.

# 27 VLAN

## 27.1 Overview

In a switched Ethernet, each port in the device is an independent collision domain, but all the ports belong to a broadcast domain. When a terminal device sends broadcast packets, all devices in the Local Area Network (LAN) can receive the packets. This not only wastes network bandwidth, but also brings hidden troubles.

Virtual Local Area Network (VLAN) is a technology through which devices in the same LAN can be divided in a logic manner. The devices in the same VLAN can communicate with each other at layer 2, while the devices from different VLANs are isolated at layer 2. In this way, broadcast packets are limited within a VLAN.

VLANs comply with IEEE 802.1Q. This standard defines a new frame encapsulation format, in which a 4-byte VLAN tag containing VLAN information is added after the source MAC address of a traditional data frame.

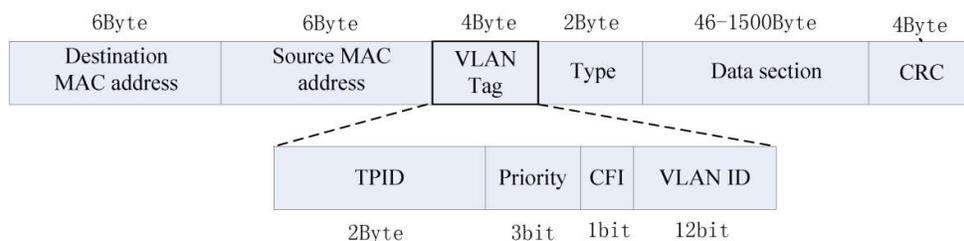


Figure 27 IEEE 802.1Q Frame Encapsulation Format

A VLAN tag contains the following four fields:

- Tag Protocol Identifier (TPID): It is used to determine whether a VLAN tag is carried by the data frame. The length is 2 bytes, and the value is fixed to be 0x8100, indicating a standard 802.1Q tag.
- Priority: It is the 802.1p priority. The length is 3 bits and the value range is 0-7. Packets with different priorities can obtain services of different levels.
- Canonical Format Indicator (CFI): It indicates whether the MAC address is encapsulated in a standard format for transmission in different media. The length is 1 bit. The value 0 indicates that the MAC address is encapsulated in a standard format while the value 1

indicates that the MAC address is encapsulated in a non-standard format.

- VLAN ID: It indicates the VLAN to which the packet belongs. The length is 12 bits, and the value range is 0-4095, where 0 and 4095 are protocol reserved values, and the available VLAN IDs are in the range of 1-4094.

VLANs have the following advantages:

- Establishes virtual workgroups flexibly. Users with the same requirements can be divided into one VLAN, without being limited by their physical locations.
- Limits broadcast domains. A VLAN is a broadcast domain. Layer-2 unicast, multicast, and broadcast frames can be forwarded only within the domain, and they cannot enter other VLANs directly. This prevents broadcast storms.
- Improves the network security. Different VLANs are isolated at layer two, and the VLANs cannot communicate with each other directly.

According to applications, VLANs are categorized into the following four types:

- Port-based VLANs
- MAC address-based VLANs
- IP subnet-based VLANs
- Protocol-based VLANs

By default, in the order of priorities from high to low, the four types of VLANs are: MAC address-based VLANs, IP subnet-based VLANs, protocol-based VLANs, and port-based VLANs. On one port, the VLAN takes effect according to the priority levels, and only one type of VLAN takes effect.

## 27.2 VLAN Function Configuration

Table 27 VLAN Function Configuration List

Configuration Task	
Configure basic attributes for VLAN	Configure VLAN
	Configure VLAN name
Configure a Port-Based VLAN	Configure the Port Link Type
	Add an Access Port into the VLAN
	Configure a Trunk Port to Allow Services of a VLAN to Pass
	Add a Hybrid Port into the VLAN

Configuration Task	
	Configure PVIDs for Ports
Configure a MAC Address-Based VLAN	Configure a MAC Address-Based VLAN
Configure an IP Subnet-Based VLAN	Configure an IP Subnet-Based VLAN
Configure a Protocol-Based VLAN	Configure a Protocol-Based VLAN
Configure the Types of Frames that Can Be Received by the Port	Configure the Types of Frames that Can Be Received by the Port

## 27.2.1 Configure basic attributes for VLAN

### Configuration Condition

None

### Configure VLAN

Each VLAN is an independent broadcast domain. Users within the same VLAN can communicate with each other in Layer 2, while those in different VLANs are isolated from each other in Layer 2.

Table 27-2 Configuring VLAN

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Create VLAN	<b>vlan</b> <i>vlan-list</i>	Mandatory By default, the system creates VLAN1 automatically. If a single VLAN is created, you will enter the VLAN configuration mode after creation. If multiple VLANs are created, you will

Step	Command	Description
		maintain in current configuration mode after creation.

### Configure VLAN name

For the convenience of memorization and management, VLAN name can be configured according to VLAN service type, function, and connection status.

Table 27-3 Configuring VLAN Name

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the VLAN configuration mode	<b>vlan <i>vlan-id</i></b>	-
Configure VLAN name	<b>name <i>vlan-name</i></b>	Mandatory  By default, the name of VLAN1 is "DEFAULT", and those of other VLANs are "VLAN <i>vlan-id</i> ", e.g. "VLAN0100".

### 27.2.2 Configure a Port-Based VLAN

A port-based VLAN, also called port VLAN, is a VLAN of the simplest division type. After a port is added into the VLAN, the port can forward packets that belong to the VLAN.

#### Configuration Condition

None

#### Configure the Port Link Type

According to the VLAN tag handling modes, the following three link types are available:

- Access type: The packets that have been forwarded do not carry VLAN tags. Ports of this type are usually connected to user devices.

- Trunk type: The packets from the VLANs in which the PVID is located do not carry VLAN tags, while the packets from other VLANs still carry VLAN tags.
- Hybrid type: The packets from the specified VLAN can be configured not to carry or carry VLAN tags. Ports of the type can be connected to user devices or interconnected with network devices.

The ports of the Trunk type and the ports of the Hybrid type cannot be converted to each other directly. They need to be converted to the Access type before being converted to another type.

Table 27-4 Configuring Link Type of Port

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Configure the Port Link Type	<b>switchport mode { access   hybrid   trunk }</b>	Mandatory  By default, the port link type is the Access type.

### Caution

- Some commands can be configured only on the ports with the specified link type. Therefore, if the port link type is converted to another type, the functions that are configured on the port with the original link type may become invalid.

## Add an Access Port into the VLAN

One Access port can belong to only one VLAN. When an Access port is added into a specified VLAN, it exits from the current VLAN and then enters the specified VLAN. If the VLAN to which the Access port is to be added does not exist, the VLAN is automatically created.

Table 27-5 Add Access Port into VLAN

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Configure the port link type as the Access type.	<b>switchport mode access</b>	Mandatory  By default, the port link type is the Access type.
Add an Access port into the specified VLAN.	<b>switchport access vlan</b> <i>vlan-id</i>	Mandatory  By default, the Access port is added into VLAN1.

### Configure a Trunk Port to Allow Services of a VLAN to Pass

If a Trunk port allows services of an existing VLAN to pass, the port allows forwarding packets of the VLAN. If the VLAN that the Trunk port allows to pass does not exist, the VLAN will not be created automatically and you must create the VLAN before the port allows forwarding packets of the VLAN.

Table 27-6 Configuring Trunk Port to Allow VLAN to Pass

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Configure the port link type as the Trunk type.	<b>switchport mode trunk</b>	Mandatory  By default, the port link type is the Access type.
Configure a Trunk port to allow a VLAN to pass.	<b>switchport trunk allowed</b> <i>vlan { all   add vlan-list }</i>	Mandatory  By default, the Trunk port allows VLAN1 to pass.
Configure the packets from the VLAN in which the PVID is located to be forwarded with VLAN tags reserved.	<b>vlan dot1q tag pvid</b>	Optional  By default, the packets from the VLAN in which the PVID is located are forwarded without VLAN tags.

### Add a Hybrid Port into the VLAN

If the VLAN to which the Access port is to be added does not exist, the VLAN is automatically created.

Table 27-7 Add Hybrid Port into VLAN

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected. After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Configure the port link type as the Hybrid type.	<b>switchport mode hybrid</b>	Mandatory By default, the port link type is the Access type.
Add a Hybrid port to a specified VLAN in a specified mode.	<b>switchport hybrid</b> { <b>untagged</b>   <b>tagged</b> } <b>vlan</b> <i>vlan-list</i>	Mandatory By default, the Hybrid port is added into VLAN1 in Untagged mode.

### Configure PVIDs for Ports

Port VLAN ID (PVID) is an important parameter of a port. When a port receives an Untag packet, it adds a VLAN tag to the packet, and the VLAN ID of the VLAN tag is the PVID of the port.

The PVID of an Access port is the ID of the VLAN to which it belongs, so the PVID of the Access port can be configured only by changing the VLAN to which it belongs. The Trunk port and hybrid port can belong to multiple VLANs, and their PVIDs can be configured according to the actual requirement.

The Trunk port and Hybrid port must be added into the VLAN to which their PVIDs belong; otherwise, packets of the VLAN to which their PVIDs belong cannot be forwarded, and the port discards the received Untag packets.

Table 27-8 Configuring PVID of Port

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected. After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Configure PVID of Trunk port	<b>switchport trunk pvid vlan</b> <i>vlan-id</i>	Mandatory, select one according to the link type of port
Configure PVID of Hybrid port	<b>switchport hybrid pvid vlan</b> <i>vlan-id</i>	By default, the port LACP is VLAN1.

---

### Note

- In configuring the PVID for a port, the VLAN to which the PVID belongs must have been created; otherwise, the configuration fails, and an error message is prompted.
- 

### 27.2.3 Configure a MAC Address-Based VLAN

MAC address-based VLANs, also called MAC VLANs, are classified according to the source MAC addresses of the packets. After a MAC VLAN is configured, if the port receives an Untag packet and the source MAC address of the packet matches a MAC VLAN entry, the system adds a VLAN tag for the packet, in which the VLAN ID matches the VLAN ID in the MAC VLAN entry.

After the physical location of the user is changed, if the MAC address of the user is not changed, the VLAN to which the user port belongs need not be re-configured.

## Configuration Condition

None

## Configure a MAC Address-Based VLAN

Table 27-9 Configuring MAC-based VLAN

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure a MAC VLAN entry.	<b>mac-vlan mac-address</b> <i>mac-address</i> <b>vlan</b> <i>vlan-id</i>	Mandatory By default, no MAC VLAN entry is configured.
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected. After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Enable the MAC VLAN function of the port.	<b>mac-vlan enable</b>	Mandatory By default, the MAC VLAN function is disabled on the port.

---

### Note

- The port on which the MAC VLAN function is enabled must be added into the VLAN that matches the entry; otherwise, the port cannot forward packets of the VLAN, and the packets that match the source MAC address will be discarded.
-

## 27.2.4 Configure an IP Subnet-Based VLAN

IP subnet-based VLANs, also called IP subnet VLANs, are classified according to the source IP addresses of the packets. After an IP subnet VLAN is configured, if the port receives an Untag packet and the source IP address of the packet matches an IP subnet VLAN entry, the system adds a VLAN tag for the packet, in which the VLAN ID matches the VLAN ID in the IP subnet VLAN entry.

After the physical location of the user is changed, if the IP address of the user is not changed, the VLAN to which the user port belongs need not be re-configured.

### Configuration Condition

None

### Configure an IP Subnet-Based VLAN

Table 27-1 Configuring IP Subnet-based VLAN

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure an IP subnet-based VLAN entry	<b>ip-subnet-vlan ipv4 ip-address mask mask vlan vlan-id</b>	Mandatory By default, no IP subnet VLAN entry is configured.
Enter the layer-2 Ethernet interface configuration mode.	<b>interface interface-name</b>	At least one option must be selected.  After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation link-aggregation-id</b>	
Enable the IP subnet VLAN function of the port	<b>ip-subnet-vlan enable</b>	Mandatory By default, the IP subnet VLAN function is disabled on the port.

---

 **Note**

- The port on which the IP subnet VLAN function is enabled must be added into the VLAN that matches the entry; otherwise, the port cannot forward packets of the VLAN, and the packets that match the source IP address will be discarded.
- 

### 27.2.5 Configure an IPV6 Subnet-based VLAN

IPV6 subnet-based VLANs, also called IPV6 subnet VLANs, are classified according to the source IPV6 addresses of the packets. After an IPV6 subnet VLAN is configured, if the port receives an Untag packet and the source IPV6 address of the packet matches an IPV6 subnet VLAN entry, the system adds a VLAN Tag for the packet, in which the VLAN ID matches that in the IPV6 subnet VLAN entry.

After the physical location of the user is changed, if the IPV6 address of the user is not changed, the VLAN to which the user port belongs need not be re-configured.

#### Configuration Condition

None

#### Configure an IPV6 Subnet-based VLAN

Table 27-11 Configuring IPV6 Subnet-based VLAN

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure an IPV6 subnet-based VLAN entry	<b>ipv6-subnet-vlan ipv6 prefix-address vlan vlan-id</b>	Mandatory By default, no IPV6 subnet VLAN entry is configured.
Enter the layer-2 Ethernet interface configuration mode.	<b>interface interface-name</b>	At least one option must be selected. After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation link-aggregation-id</b>	After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent

Step	Command	Description
		configuration takes effect only within the aggregation group.
Enable the IPV6 subnet VLAN function of the port	<b>ipv6-subnet-vlan enable</b>	Mandatory  By default, the IPV6 subnet VLAN function is disabled on the port.

### Note

- The port on which the IPV6 subnet VLAN function is enabled must be added into the VLAN that matches the entry; otherwise, the port cannot forward packets of the VLAN, and the packets that match the source IPV6 address will be discarded.

## 27.2.6 Configure a Protocol-Based VLAN

Protocol-based VLANs, also called protocol VLANs, are classified according to the frame encapsulation formats and protocol types of packets. After a protocol profile is defined, a port is configured to match a protocol profile, and the protocol VLAN function is enabled for the port, if the port receives an Untag packet that matches the protocol profile, the port adds a VLAN tag for the packet. The VLAN ID matches the VLAN ID defined in the profile.

After the physical location of the user is changed, if the frame encapsulation format of the user packets and protocol type are not changed, the VLAN to which the user port belongs need not be re-configured.

### Configuration Condition

None

### Configure a Protocol-Based VLAN

Table 27-12 Configuring Protocol-based VLAN

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Define protocol profile	<b>protocol-vlan profile</b> <i>profile-index frame-type</i> <i>frame-type ether-type</i> <i>ether-type</i>	Mandatory  By default, the protocol profile is not defined.
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Configure the protocol profile that matches the port	<b>protocol-vlan profile</b> <i>profile-index vlan</i> <i>vlan-id</i>	Mandatory  By default, the port doesn't match any protocol profile.
Enable the protocol VLAN function of the port	<b>protocol-vlan enable</b>	Mandatory  By default, the protocol VLAN function is disabled on the port.

---

### Note

- The port for which a matching protocol profile has been configured and the protocol VLAN function has been enabled must be added into the VLAN corresponding to the protocol profile that it matches; otherwise, the port cannot forward packets of the VLAN, and the packets matching the protocol will be discarded.
- 

## 27.2.7 Configure the Types of Frames that Can Be Received by the Port

### Configuration Condition

None

### Configure the Types of Frames that Can Be Received by the Port

You can configure the types of frames that can be received by a port so that the port receives only Untag packets, receives only Tag packets, or receives both of them. The packets that fail to meet the requirement will be discarded.

Table 27-13 Configuring the Types of Frames that Can be Received by the Port

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Configure the Types of Frames that Can Be Received by the Port	<b>switchport accept frame-type { all   untag   tag }</b>	Mandatory  By default, the type of frames that can be received by a port is all, that is, receiving both Untag and Tag packets.

## 27.2.8 VLAN Monitoring and Maintaining

Table 27-14 VLAN Monitoring and Maintaining

Command	Description
<b>show ip-subnet-vlan</b>	Show the information of IP subnet VLAN

Command	Description
<b>show ipv6-subnet-vlan</b>	Show the information of IPV6 subnet VLAN
<b>show mac-vlan</b>	Show the information of MAC VLAN
<b>show protocol-vlan [ profile ]</b>	Show the information of protocol VLAN
<b>show running-config vlan</b>	Show the information of VLAN configuration
<b>show vlan [ vlan-id ]</b>	Show the information of specified VLAN or all created VLAN
<b>show vlan statistics</b>	Show the number of created VLANs
<b>show vlan summary</b>	Show the VLAN information of static creation and dynamic learning
<b>show { interface interface-name   interface link-aggregation link-aggregation-id } vlan status</b>	Show the VLAN information of specified port or aggregation group

## 27.3 VLAN Typical Configuration Example

### 27.3.1 Configure a Port-Based VLAN

#### Network Requirements

- Server1 and PC1 are in the office network, while Server2 and PC2 are in the production network.
- You need to configure the port-based VLAN functions to isolate PC1 and PC2 so that PC1 can access only Server1 and PC2 can access only Server2.

#### Network Topology

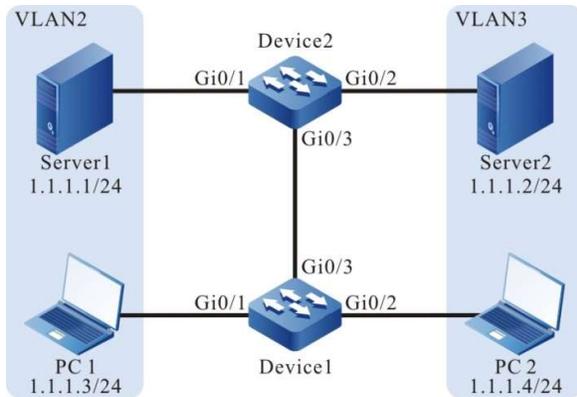


Figure 27 Configuring Network Topology of VLAN based on Port

### Configuration Steps

*Step 1:* Configure VLAN and port link type on Device1.

#Create VLAN2 and VLAN3 on Device1.

```
Device1#configure terminal
Device1(config)#vlan 2-3
```

#Configure the link type of ports gigabitethernet0/1 and gigabitethernet0/2 on Device1 as Access. Port gigabitethernet0/1 allows the pass of services of VLAN2 while port gigabitethernet0/2 allows the pass of services of VLAN3.

```
Device1(config)#interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#switchport mode access
Device1(config-if-gigabitethernet0/1)#switchport access vlan 2
Device1(config-if-gigabitethernet0/1)#exit
Device1(config)#interface gigabitethernet0/2
Device1(config-if-gigabitethernet0/2)#switchport mode access
Device1(config-if-gigabitethernet0/2)#switchport access vlan 3
Device1(config-if-gigabitethernet0/2)#exit
```

#On Device1, configure the link type of port gigabitethernet0/3 as Trunk, and allow the pass of services of VLAN2 and VLAN3.

```
Device1(config)#interface gigabitethernet 0/3
Device1(config-if-gigabitethernet0/3)#switchport mode trunk
Device1(config-if-gigabitethernet0/3)#switchport trunk allowed vlan add 2-3
Device1(config-if-gigabitethernet0/3)#exit
```

*Step 2:* Configure VLAN and port link type on Device2.

#Create VLAN2 and VLAN3 on Device2.

```
Device2#configure terminal
Device2(config)#vlan 2-3
```

#Configure the link type of port gigabitethernet0/1 and gigabitethernet0/2 on Device2 as Access. Port gigabitethernet0/1 allows the services of VLAN2 to pass and gigabitethernet0/2 allows the services of VLAN3 to pass.

```
Device2(config)#interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#switchport mode access
Device2(config-if-gigabitethernet0/1)#switchport access vlan 2
Device2(config-if-gigabitethernet0/1)#exit
Device2(config)#interface gigabitethernet0/2
Device2(config-if-gigabitethernet0/2)#switchport mode access
Device2(config-if-gigabitethernet0/2)#switchport access vlan 3
Device2(config-if-gigabitethernet0/2)#exit
```

#On Device2, configure the link type of port gigabitethernet0/3 as Trunk, and allow services of VLAN2 and VLAN3 to pass.

```
Device2(config)#interface gigabitethernet 0/3
Device2(config-if-gigabitethernet0/3)#switchport mode trunk
Device2(config-if-gigabitethernet0/3)#switchport trunk allowed vlan add 2-3
Device2(config-if-gigabitethernet0/3)#exit
```

*Step*  
3:

Check the result.

#View the information of VLAN on Device1.

```
Device1#show vlan 2
-----
NO. VID VLAN-Name          Owner Mode  Interface
-----
1  2  VLAN0002                static Tagged gi0/3
                               Untagged gi0/1
Device1#show vlan 3
-----
NO. VID VLAN-Name          Owner Mode  Interface
-----
1  3  VLAN0003                static Tagged gi0/3
                               Untagged gi0/2
```

#View the information of VLAN on Device2.

```
Device2#show vlan 2
-----
NO. VID VLAN-Name          Owner Mode  Interface
-----
1  2  VLAN0002                static Tagged gi0/3
                               Untagged gi0/1
Device2#show vlan 3
-----
NO. VID VLAN-Name          Owner Mode  Interface
-----
1  3  VLAN0003                static Tagged gi0/3
                               Untagged gi0/2
```

# PC1 and PC2 cannot communicate with each other. PC1 can access Server1 only, and PC2 can access Server2 only.

## 27.3.2 Configure a MAC Address-Based VLAN

### Network Requirements

User manual  
Release 1.0 01/2022

- PC1 and PC2 can access the network through different ports of Device.
- The MAC-address based VLAN functions need to be configured so that the PCs with the specified MAC addresses can access the server through different ports. PCs which do not have a specified MAC address can access the server only through a specified port.

## Network Topology

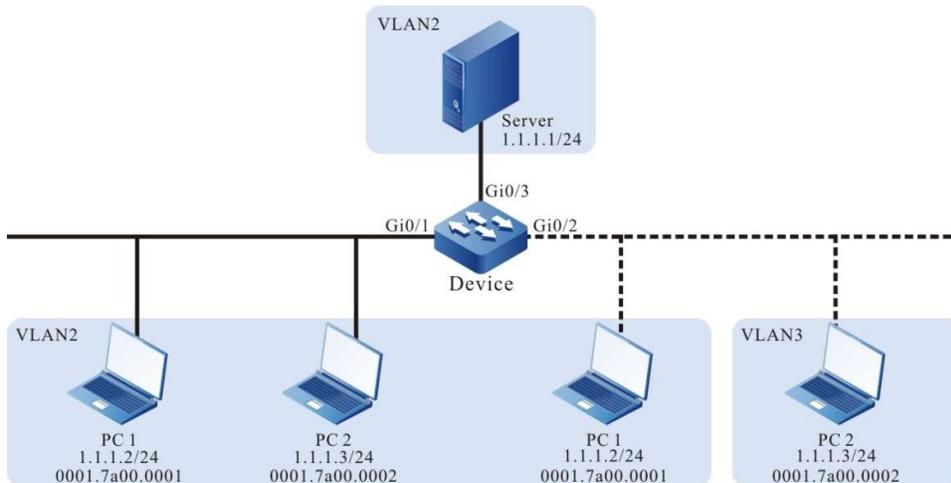


Figure 1 Configure Network Topology of VLAN based on MAC

## Configuration Steps

*Step 1:* Configure VLAN and port link type on Device.

Create VLAN2 and VLAN3 on Device.

```
Device#configure terminal
Device(config)#vlan 2-3
```

#Configure the link type of ports gigabitethernet0/1 and gigabitethernet0/3 on Device as Access, allowing the services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/1,0/3
Device(config-if-range)#switchport mode access
Device(config-if-range)#switchport access vlan 2
Device(config-if-range)#exit
```

#On Device, configure the link type of port gigabitethernet0/2 as Hybrid, and allow services of VLAN2 and VLAN3 to pass. PVID is 3.

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode hybrid
Device(config-if-gigabitethernet0/2)#switchport hybrid untagged vlan 2-3
Device(config-if-gigabitethernet0/2)#switchport hybrid pvid vlan 3
Device(config-if-gigabitethernet0/2)#exit
```

*Step*  
*2:*           Configure a MAC-based VLAN function.

#Configure a MAC-based VLAN entry on the Device so that the packet with the source MAC address of 0001.7a00.0001 is forwarded in VLAN 2.

```
Device(config)#mac-vlan mac-address 0001.7a00.0001 vlan 2
```

#On the port gigabitethernet0/2 of the Device, enable MAC-based VLAN functions.

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#mac-vlan enable
Device(config-if-gigabitethernet0/2)#exit
```

*Step*  
*3:*           Check the result.

#On the Device, view the information of MAC VLAN entry and the enabling status of port.

```
Device#show mac-vlan
                total 1024,  used 1,  left 1023

-----MAC-VLAN-----
NO.  Mac Address  Dynamic Vlan  Static Vlan  Current Pri  Static Pri
-----
1    0001.7a00.0001  0           2           -           -

-----ENABLE MAC-VLAN-----
gi0/2
```

#PC1 can access the server when connected from port gigabitethernet0/1 or gigabitethernet0/2, and PC2 can access the server only when connected from port gigabitethernet0/1.

### 27.3.3 Configure an IP Subnet-Based VLAN

#### Network Requirements

- Server1 is an office network server, while Server2 is a production network server.
- You need to configure the IP subnet-based VLAN functions so that PC1 can access Server1 only and PC2 can access Server2 only.

#### Network Topology

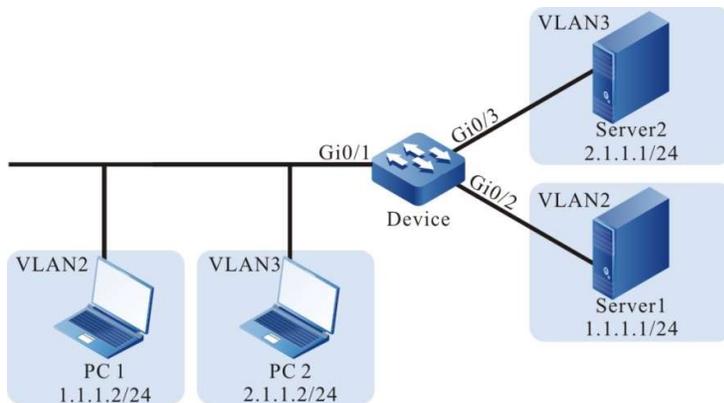


Figure 2 Configure Network Topology for IP Subnet-based VLAN

### Configuration Steps

*Step 1:* Configure VLAN and port link type on Device.

#Create VLAN2 and VLAN3 on Device.

```
Device#configure terminal
Device(config)#vlan 2-3
```

#On Device, configure the link type of port gigabitethernet0/1 as Hybrid, and allow services of VLAN2 and VLAN3 to pass. PVID is 2.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode hybrid
Device(config-if-gigabitethernet0/1)#switchport hybrid untagged vlan 2-3
Device(config-if-gigabitethernet0/1)#switchport hybrid pvid vlan 2
Device(config-if-gigabitethernet0/1)#exit
```

#Configure the link type of ports gigabitethernet0/2 and gigabitethernet0/3 on Device as Access. Port gigabitethernet0/2 allows the services of VLAN2 to pass and gigabitethernet0/3 allows the services of VLAN3 to pass.

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode access
Device(config-if-gigabitethernet0/2)#switchport access vlan 2
Device(config)#interface gigabitethernet 0/3
Device(config-if-gigabitethernet0/3)#switchport mode access
Device(config-if-gigabitethernet0/3)#switchport access vlan 3
Device(config-if-gigabitethernet0/3)#exit
```

*Step 2:* Configure an IP subnet-based VLAN function.

#Configure an IP subnet-based VLAN entry on the Device so that the packet with the source IP address belonging to the 2.1.1.0/24 network segment is forwarded in VLAN 3.

```
Device(config)#ip-subnet-vlan ipv4 2.1.1.0 mask 255.255.255.0 vlan 3
```

#On the port gigabitethernet0/1 of the Device, enable IP subnet-based VLAN functions.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#ip-subnet-vlan enable
Device(config-if-gigabitethernet0/1)#exit
```

Step  
3:

Check the result.

#On the Device, view the information of IP subnet VLAN entry and the enabling status of port.

```
Device(config)#show ip-subnet-vlan
-----IP-SUBNET-VLAN-----
NO.  IP      MASK      VLAN  PRI
-----
1    2.1.1.0  255.255.255.0  3    -

-----Enable SUBNET-VLAN-----
gi0/1

-----Enable SUBNET-VLAN Priority-----
```

# PC1 can access Server1 only, and PC2 can access Server2 only.

## 27.3.4 Configure an IPV6 Subnet-based VLAN

### Network Requirements

- Server1 is an office network server, while Server2 is a production network server.
- You need to configure the IPV6 subnet-based VLAN functions so that PC1 can access Server1 only and PC2 can access Server2 only.

### Network Topology

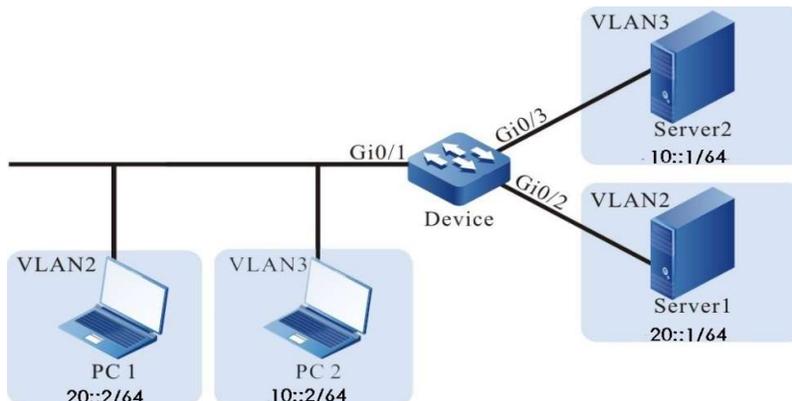


Figure 3 Configuring Network Topology for IPv6 Subnet-based VLAN

### Configuration Steps

*Step*  
*1:*           Configure VLAN and port link type on Device.

#Create VLAN2 and VLAN3 on Device.

```
Device#configure terminal
Device(config)#vlan 2-3
```

#On Device, configure the link type of port gigabitethernet0/1 as Hybrid, and allow services of VLAN2 and VLAN3 to pass. PVID is 2.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode hybrid
Device(config-if-gigabitethernet0/1)#switchport hybrid untagged vlan 2-3
Device(config-if-gigabitethernet0/1)#switchport hybrid pvid vlan 2
Device(config-if-gigabitethernet0/1)#exit
```

#Configure the link type of ports gigabitethernet0/2 and gigabitethernet0/3 on Device as Access. Port gigabitethernet0/2 allows the services of VLAN2 to pass and gigabitethernet0/3 allows the services of VLAN3 to pass.

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode access
Device(config-if-gigabitethernet0/2)#switchport access vlan 2
Device(config)#interface gigabitethernet 0/3
Device(config-if-gigabitethernet0/3)#switchport mode access
Device(config-if-gigabitethernet0/3)#switchport access vlan 3
Device(config-if-gigabitethernet0/3)#exit
```

*Step*  
*2:*           Configure an IPV6 subnet-based VLAN function.

#Configure an IPV6 subnet-based VLAN entry on the Device so that the packet with the source IPV6 address belonging to the 10::1/64 network segment is forwarded in VLAN 3.

```
Device(config)# ipv6-subnet-vlan ipv6 10::1/64 vlan 3
```

#On the port gigabitethernet0/1 of the Device, enable IPV6 subnet-based VLAN functions.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#ipv6-subnet-vlan enable
Device(config-if-gigabitethernet0/1)#exit
```

*Step*  
*3:*           Check the result.

#On the Device, view the information of IPV6 subnet VLAN entry and the enabling status of port.

```
Device(config)#show ipv6-subnet-vlan
-----IPV6-SUBNET-VLAN-----
NO. IPV6                VLAN  PRI
1  10::/64                3     -
-----Enable SUBNET-VLAN-----
gi0/1
```

# PC1 can access Server1 only, and PC2 can access Server2 only.

## 27.3.5 Configure a Protocol-Based VLAN

### Network Requirements

- In Ethernet, PC is a host, while Server1 and Server2 are two servers.
- Configure protocol-based VLAN functions so that when the protocol-based VLAN functions are not enabled by the port on the Device, PC can only access Server1; when the port enables the protocol-based VLAN function, PC can only access Server2.

### Network Topology

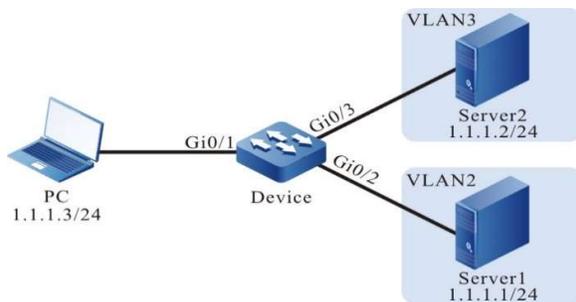


Figure 4 Configuring Network Topology of VLAN based on Protocol

### Configuration Steps

*Step 1:* Configure VLAN and port link type on Device.

#Create VLAN2 and VLAN3 on Device.

```
Device#configure terminal
Device(config)#vlan 2-3
```

#On Device, configure the link type of port gigabitethernet0/1 as Hybrid, and allow services of VLAN2 and VLAN3 to pass. PVID is VLAN 2.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport hybrid untagged vlan 2-3
Device(config-if-gigabitethernet0/1)#switchport hybrid pvid vlan 2
```

#Configure the link type of ports gigabitethernet0/2 and gigabitethernet0/3 on Device as Access. Port gigabitethernet0/2 allows the services of VLAN2 to pass and gigabitethernet0/3 allows the services of VLAN3 to pass.

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode access
Device(config-if-gigabitethernet0/2)#switchport access vlan 2
Device(config-if-gigabitethernet0/2)#exit
Device(config)#interface gigabitethernet 0/3
Device(config-if-gigabitethernet0/3)#switchport mode access
Device(config-if-gigabitethernet0/3)#switchport access vlan 3
Device(config-if-gigabitethernet0/3)#exit
```

*Step*  
2:           Configure a protocol-based VLAN function.

#Configure protocol profile based on the ETHERII encapsulated IP (0x0800) packet on the Device.

```
Device(config)#protocol-vlan profile 1 frame-type ETHERII ether-type 0x0800
```

#Apply the packet matching the protocol profile mentioned above on the port gigabitethernet0/1 of Device to be forwarded in VLAN 3, and enable the protocol VLAN function.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#protocol-vlan profile 1 vlan 3
Device(config-if-gigabitethernet0/1)#protocol-vlan enable
Device(config-if-gigabitethernet0/1)#exit
```

*Step*  
3:           Check the result.

#On the Device, view the information of protocol VLAN entry and the enabling status of port.

```
Device#show protocol-vlan profile
-----PROTOCOL-VLAN-TEMPLATE-----
Profile  Frame-type  Ether-type
-----
1      ETHERII      0x800

-----Enable PROTOCOL-VLAN-----
gi0/1

-----Enable PROTOCOL-VLAN Profile-----
gi0/1: total-profiles 1
      vlan 3, profile 1
Device#show protocol-vlan
-----PROTOCOL-VLAN-----
Interface      Profile      VLAN
-----
gi0/1          1            3

-----Enable PROTOCOL-VLAN-----
gi0/1

-----Enable PROTOCOL-VLAN Profile-----
gi0/1: total-profiles 1
      vlan 3, profile 1
```

#When the port gigabitethernet0/1 fails to enable the protocol-based VLAN functions, PC can only access Server1; when the port gigabitethernet0/1 enables the protocol-based VLAN function, PC can only access Server2.

# 28 QinQ and VLAN Mapping

## 28.1 Overview

QinQ (802.1Q in 802.1Q) is the extension based on 802.1Q protocol. It adds a layer of 802.1Q tag (VLAN Tag) to the original 802.1Q packet header to increase the number of VLAN to 4094×4094 through double layers of VLAN Tag. QinQ encapsulates the user's private network VLAN Tag in the public network VLAN Tag so that the packet can transmit in the backbone network (public network) of the operator with double layers of VLAN Tag. In the public network, the packet only spreads according to outer VLAN Tag (i.e. VLAN Tag of public network). Users' private network VLAN Tags are shielded. This saves VLAN ID of public network and provides users with a simple two-payer VPN (Virtual Private Network) tunnel.

QinQ can be divided into the following types according to the rules of adding VLAN Tag:

- Basic QinQ;
- Port-based flexible QinQ.

VLAN mapping is also the extension based on 802.1Q protocol. It is different from QinQ. Instead of encapsulating a layer of VLAN Tag based on the original VLAN Tag of the packet, VLAN mapping replaces the original VLAN Tag of the packet with a new one. This means the packet still has only one layer of VLAN Tag.

VLAN mapping can be divided into the following types by mapping rules:

- 1: 1 VLAN mapping. This means only a private network VLAN is mapped to a public network VLAN;
- N: 1 VLAN mapping. This means one or more private network VLANs can be mapped to a public network VLAN.

The port-based flexible QinQ, 1:1 VLAN mapping and N:1 VLAN mapping all need to be configured with mapping entries from private network VLAN to public network VLAN. Users can configure 4096 mapping entries at most.

## 28.2 QinQ and VLAN mapping function configuration

Table 1 QinQ and VLAN Mapping Function Configuration List

Configuration Task	
Configure basic QinQ function	Enable basic QinQ function

Configuration Task	
Configure port-based flexible QinQ function	Configure port-based flexible QinQ function
Configure 1: 1 VLAN mapping function	Configure 1: 1 VLAN mapping function
Configure N: 1 VLAN mapping function	Configure N: 1 VLAN mapping function
Configure the protocol type of outer VLAN Tag of the port	Configure the protocol type of outer VLAN Tag of the port
Configure QinQ Drop function	Enable QinQ Drop function
Configure QinQ port isolation function	Configure function of QinQ-related mutual isolation of ports

### 28.2.1 Configure basic QinQ function

After the port is configured with the basic QinQ function, the device adds a layer of VLAN tag to the packets received by the port. The VLAN ID of VLAN tag is the PVID of the port.

#### Configuration Condition

Before configuring the basic QinQ function, the following tasks should be completed:

- Configure PVID of port, which is the VLAN ID of outer VLAN Tag added after the port enables basic QinQ.

#### Enable basic QinQ function

Table 4- 2 Enabling Basic QinQ Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2 Ethernet interface configuration mode, the

Step	Command	Description
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enable basic QinQ function	<b>vlan dot1q-tunnel enable</b>	Mandatory  By default, the basic QinQ function is disabled.

---

### Note

- Under the same port, the basic QinQ function cannot be used with the following functions: QinQ Evc, flexible QINQ, 1:1 VLAN mapping, N:1 VLAN mapping, and configure the protocol type of outer VLAN Tag of the port as a non-default value.
- 

## 28.2.2 Configure port-based flexible QinQ function

After the port is configured with port-based flexible QinQ, if the VLAN ID of the outermost VLAN tag of the packet matches the port-based flexible QinQ entry, the specified outer VLAN tag is added to the packet; if the VLAN ID of the packet's outermost VLAN Tag does not match the port-based flexible QinQ entry, the flexible QINQ will not process this packet.

### Configuration Condition

Before configuring the port-based flexible QinQ function, the following tasks should be completed:

- Configure the port link type as Trunk or Hybrid;
- Configure PVID of port;
- Configure the port with the VLAN of the added outer VLAN Tag to ensure that the packet with outer VLAN Tag can pass.

### Configure port-based flexible QinQ function

Table 28 Configuring Port-based Flexible QinQ Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.
Enter Aggregation Group Configuration Mode	<b>link-aggregation</b> <i>link-aggregation-id</i>	After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Configure port-based flexible QinQ entry	<b>vlan dot1q-tunnel</b> <i>inner-vlan-list outer-vlan-id</i>	Mandatory  By default, the port-based flexible QinQ entry is not configured.

---

### Note

- Under the same port, the port-based flexible QinQ function cannot be used with the following functions: QinQ Evc, basic QINQ, 1:1 VLAN mapping, and N:1 VLAN mapping.
  - When the configured port-based flexible QinQ entry conflicts with the existing one on the port, a prompt of conflict will be given.
-

### 28.2.3 Configure 1:1 VLAN mapping function

For a port, 1:1 VLAN mapping entries only have a one-to-one relationship with each other, which means only one private network VLAN can be mapped to one public network VLAN.

After the port is configured with 1:1 VLAN mapping, if the VLAN ID of the packet's outermost VLAN Tag matches the entry of the 1:1 VLAN mapping, the VLAN ID of the packet's outermost VLAN Tag will be replaced with the specified VLAN ID; otherwise, the 1:1 VLAN mapping will not process the packet.

#### Configuration Condition

Before configuring the 1:1 VLAN mapping function, the following tasks should be completed:

- Configure the port link type as Trunk or Hybrid;
- Configure PVID of port;
- Configure the port with the VLAN of the new outer VLAN Tag to ensure that the packet with outer VLAN Tag being replaced can pass.

#### Configure 1:1 VLAN mapping function

Table 2 Configuring 1:1 VLAN Mapping Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected. After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only
Enter Aggregation Group Configuration Mode	<b>link-aggregation</b> <i>link-aggregation-id</i>	

Step	Command	Description
		within the aggregation group.
Configure 1:1 VLAN mapping entry	<b>vlan dot1q-tunnel mapping</b> <i>former-vlan-id mapping-vlan-id</i>	Mandatory  By default, no 1: 1 VLAN mapping entry is configured.

---

### Note

- Under the same port, the 1: 1 VLAN mapping function cannot be used with the following functions: QinQ Evc, basic QINQ, flexible QINQ, and N:1 VLAN mapping.
  - When the configured 1: 1 VLAN mapping entry conflicts with the existing port-based one on the port, a prompt of conflict will be given.
- 

## 28.2.4 Configure N: 1 VLAN mapping function

For a port, multiple N:1 VLAN mapping entries can be configured. They may have a many-to-one relationship with each other, which means one or more private network VLANs can be mapped to one public network VLAN.

After the port is configured with N:1 VLAN mapping, if the VLAN ID of the outermost VLAN tag of the packet matches the N:1 VLAN mapping entry, the VLAN ID of the packet's outermost VLAN Tag is replaced with the specified VLAN ID; otherwise, the N:1 VLAN mapping will not process this packet.

### Configuration Condition

Before configuring the N:1 VLAN mapping function, the following tasks should be completed:

- Configure the port link type as Trunk or Hybrid;
- Configure the port with the VLAN of the new outer VLAN Tag to ensure that the packet with outer VLAN Tag being replaced can pass.

### Configure N: 1 VLAN mapping function

Table 3 Configuring N:1 VLAN Mapping Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.
Enter Aggregation Group Configuration Mode	<b>link-aggregation</b> <i>link-aggregation-id</i>	After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enable N: 1 VLAN mapping function	<b>vlan dot1q-tunnel mapping n-to-1 enable</b>	Mandatory  By default, the N: 1 VLAN mapping function is not enabled.
Configure N:1 VLAN mapping entry	<b>vlan dot1q-tunnel mapping n-to-1</b> <i>former-vlan-list mapping-vlan-id</i>	Mandatory  By default, no N: 1 VLAN mapping entry is configured.

## Note

- Under the same port, the N: 1 VLAN mapping function cannot be used with the following functions: QinQ Evc, basic QINQ, port-based flexible QinQ, 1:1 VLAN mapping, and

---

configure the protocol type of outer VLAN Tag of the port as a non-default value.

- When the port link type is configured as Trunk, pvid cannot be the public network vlan mapped by N: 1 VLAN mapping.
  - When the port link type is configured as Hybrid, the public network vlan mapped by N: 1 VLAN mapping cannot be added in untag manner.
- 

## 28.2.5 Configure the protocol type of outer VLAN Tag of the port

The port can identify whether the packet carries corresponding VLAN Tag according to the TPID (Tag Protocol Identifier) value: when the port receives the packet, if the TPID value configured for the port is consistent with the corresponding field in the packet, it means that the packet has carried corresponding VLAN Tag; otherwise, the device deems the received packet as Untag.

Some manufacturers' devices may set the TPID field of the outer VLAN Tag of the QinQ packet as 0x9100 or other values. In order to become compatible with these devices, the TPID value of the outer VLAN Tag of this device's port should be configured as an equal value.

### Configuration Condition

None

### Configure the protocol type of outer VLAN Tag of the port

The device supports 2 different TPID configurations. The TPID configured ranging from 0x0001 to 0xffff shall not be reserved protocol fields, such as 0x0806 and 0x0800.

Table 4 Configuring Protocol Type for Outer VLAN Tag of Port

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected. After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you
Enter Aggregation Group Configuration Mode	<b>link-aggregation</b> <i>link-aggregation-id</i>	

Step	Command	Description
		enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Configure the protocol type of outer VLAN Tag of the port	<b>frame-tag tpid</b> <i>type-value</i>	Optional By default, the protocol type of outer VLAN Tag of the port is 0x8100.

### Note

- Under the same port, the operation of configuring protocol type for the outer VLAN Tag of port cannot be used with the following functions: QinQ Evc, basic QINQ, flexible QINQ, 1:1 VLAN mapping, and N:1 VLAN mapping.

## 28.2.6 Configure QinQ Drop function

After the port is configured with QinQ Drop function, if the port receives the packet which doesn't match port-based flexible QinQ entry, 1:1 VLAN mapping entry and N:1 mapping entry, it will discard it.

### Configuration Condition

Before configuring the QinQ Drop function, the following tasks should be completed:

- Configure port-based flexible QinQ, 1:1 VLAN mapping, and N:1 VLAN mapping.

### Enable QinQ Drop function

Table 28 Enabling QinQ Drop Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.
Enter Aggregation Group Configuration Mode	<b>link-aggregation</b> <i>link-aggregation-id</i>	After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enable QinQ Drop function	<b>vlan dot1q-tunnel drop</b>	Mandatory  By default, the QinQ Drop function is disabled.

---

 **Note**

- Under the same port, QinQ Drop shall not be used with QinQ Evc.
- 

## 28.2.7 QinQ and VLAN mapping monitoring and maintaining

Table 28 QinQ and VLAN Mapping Monitoring and Maintaining

Command	Description
<b>show vlan dot1q-tunnel</b>	Show port-based flexible QinQ configuration
<b>show vlan dot1q-tunnel mapping</b>	Show 1: 1 VLAN mapping configuration
<b>show vlan dot1q-tunnel mapping n-to-1 configuration</b>	Show N: 1 VLAN mapping configuration

## 28.3 Example of typical QinQ and VLAN mapping configuration

### 28.3.1 Configure basic QinQ

#### Network Requirements

- Intranet users CE1 and CE2, CE3 and CE4 communicate through the operator's network. CE1 and CE2 use intranet VLAN 10 - VLAN 20, while CE3 and CE4 use intranet VLAN 15 - VLAN 30. PE1 and PE2 are edge devices for the operator's network.
- Configure basic QinQ on PE1 and PE2 so that CE1 and CE2 communicate with each other through the operator's public network VLAN 100, and CE3 and CE4 communicate with each other through VLAN 101. The data has double layers of Tag when transmitting on the operator's network.

#### Network Topology

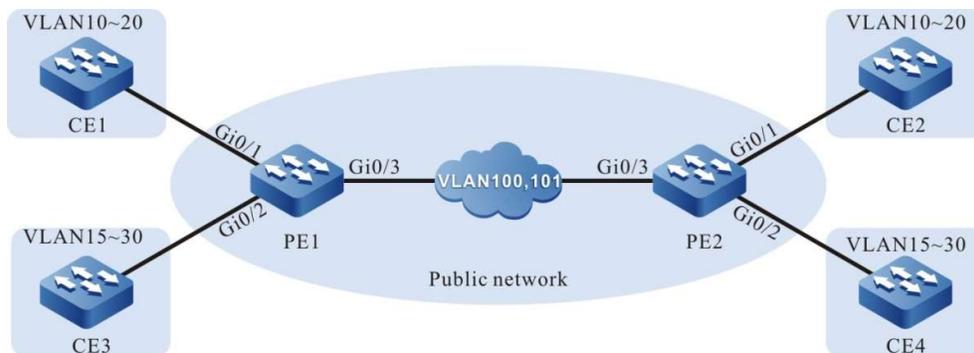


Figure 28 Configuring Network Topology of Basic QinQ

#### Configuration Steps

Step 1: Configure PE1.

#Create VLAN10~VLAN30 and VLAN100~VLAN101 on PE1.

```
PE1#configure terminal
PE1(config)#vlan 10-30,100-101
```

#On PE1, configure the link type of port gigabitethernet0/1 as Trunk, and allow services of VLAN10~VLAN20 and VLAN100 to pass. Configure PVID as 100.

```
PE1(config)#interface gigabitethernet 0/1
PE1(config-if-gigabitethernet0/1)#switchport mode trunk
PE1(config-if-gigabitethernet0/1)#switchport trunk allowed vlan add 10-20,100
PE1(config-if-gigabitethernet0/1)#switchport trunk pvid vlan 100
PE1(config-if-gigabitethernet0/1)#exit
```

#On PE1, configure the link type of port tengigabitethernet0/2 as Trunk, and allow services of VLAN15~VLAN30 and VLAN101 to pass. Configure PVID as 101.

```
PE1(config)#interface gigabitethernet 0/2
PE1(config-if-gigabitethernet0/2)#switchport mode trunk
PE1(config-if-gigabitethernet0/2)#switchport trunk allowed vlan add 15-30,101
PE1(config-if-gigabitethernet0/2)#switchport trunk pvid vlan 101
PE1(config-if-gigabitethernet0/2)#exit
```

#On PE1, configure the link type of port tengigabitethernet0/3 as Trunk, and allow services of VLAN100 and VLAN101 to pass. Configure PVID as 1.

```
PE1(config)#interface gigabitethernet0/3
PE1(config-if-gigabitethernet0/3)#switchport mode trunk
PE1(config-if-gigabitethernet0/3)#switchport trunk allowed vlan add 100,101
PE1(config-if-gigabitethernet0/3)#switchport trunk pvid vlan 1
PE1(config-if-gigabitethernet0/3)#exit
```

#On ports gigabitethernet0/1 and gigabitethernet0/2 of PE1, enable basic QinQ function.

```
PE1(config)#interface gigabitethernet 0/1
PE1(config-if-gigabitethernet0/1)#vlan dot1q-tunnel enable
PE1(config-if-gigabitethernet0/1)#exit
PE1(config)#interface gigabitethernet 0/2
PE1(config-if-gigabitethernet0/2)#vlan dot1q-tunnel enable
PE1(config-if-gigabitethernet0/2)#exit
```

Step 2: Configure PE2.

#Create VLAN10~VLAN30 and VLAN100~VLAN101 on PE2.

```
PE2#configure terminal
PE2(config)#vlan 10-30,100-101
```

#On PE2, configure the link type of port gigabitethernet0/1 as Trunk, and allow services of VLAN10~VLAN20 and VLAN100 to pass. Configure PVID as 100.

```
PE2(config)#interface gigabitethernet 0/1
PE2(config-if-gigabitethernet0/1)#switchport mode trunk
PE2(config-if-gigabitethernet0/1)#switchport trunk allowed vlan add 10-20,100
PE2(config-if-gigabitethernet0/1)#switchport trunk pvid vlan 100
PE2(config-if-gigabitethernet0/1)#exit
```

#On PE2, configure the link type of port gigabitethernet0/2 as Trunk, and allow services of VLAN15~VLAN30 and VLAN101 to pass. Configure PVID as 101.

```
PE2(config)#interface gigabitethernet 0/2
PE2(config-if-gigabitethernet0/2)#switchport mode trunk
PE2(config-if-gigabitethernet0/2)#switchport trunk allowed vlan add 15-30,101
PE2(config-if-gigabitethernet0/2)#switchport trunk pvid vlan 101
PE2(config-if-gigabitethernet0/2)#exit
```

#On PE2, configure the link type of port gigabitEthernet0/3 as Trunk, and allow services of VLAN100 and VLAN101 to pass. Configure PVID as 1.

```
PE2(config)#interface gigabitEthernet 0/3
PE2(config-if-gigabitEthernet0/3)#switchport mode trunk
PE2(config-if-gigabitEthernet0/3)#switchport trunk allowed vlan add 100,101
PE2(config-if-gigabitEthernet0/3)#switchport trunk pvid vlan 1
PE2(config-if-gigabitEthernet0/3)#exit
```

#On ports gigabitEthernet0/1 and gigabitEthernet0/2 of PE2, enable basic QinQ function.

```
PE2(config)#interface gigabitEthernet 0/1
PE2(config-if-gigabitEthernet0/1)#vlan dot1q-tunnel enable
PE2(config-if-gigabitEthernet0/1)#exit
PE2(config)#interface gigabitEthernet 0/2
PE2(config-if-gigabitEthernet0/2)#vlan dot1q-tunnel enable
PE2(config-if-gigabitEthernet0/2)#exit
```

Step 3: Check the result.

#Services between intranet users CE1 and CE2 can communicate on the operator's network VLAN100 through PE1 and PE2 with double layers of Tag; those between CE3 and CE4 can communicate on the operator's network VLAN101 through PE1 and PE2 with double layers of Tag.

### 28.3.2 Configure flexible QinQ

#### Network Requirements

- Intranet users CE1 and CE2, CE3 and CE4 communicate through the operator's network. CE1 and CE2 use intranet VLAN 10 - VLAN 20, while CE3 and CE4 use intranet VLAN 15 - VLAN 30. PE1 and PE2 are edge devices for the operator's network.
- Configure flexible QinQ rules on PE1 and PE2 so that CE1 and CE2, CE3 and CE4 can communicate with each other through the operator's public network VLAN 100 and VLAN101. The data has double layers of Tag when transmitting on the operator's network.

#### Network Topology

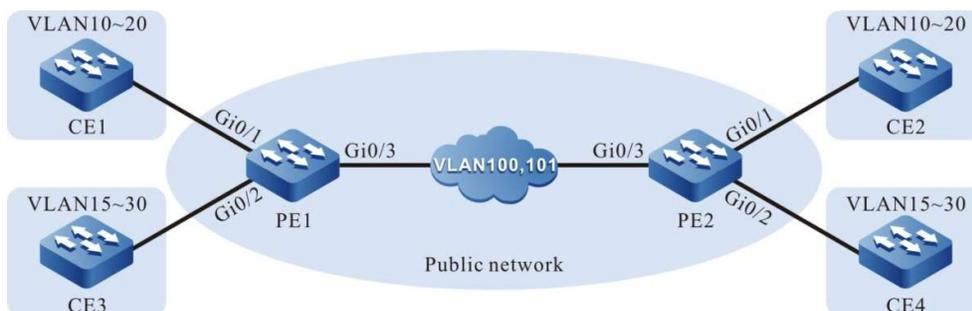


Figure 1 Configuring Network Topology of Flexible QinQ

#### Configuration Steps

**Step 1: Configure PE1.**

#Create VLAN 10~VLAN30 and VLAN100~VLAN101 on PE1.

```
PE1#configure terminal
PE1(config)#vlan 10-30,100-101
```

#On PE1, configure the link type of port gigabitethernet0/1 as Trunk, and allow services of VLAN10~VLAN20 and VLAN100 to pass. Configure PVID as 1.

```
PE1(config)#interface gigabitethernet 0/1
PE1(config-if-gigabitethernet0/1)#switchport mode trunk
PE1(config-if-gigabitethernet0/1)#switchport trunk allowed vlan add 10-20,100
PE1(config-if-gigabitethernet0/1)#switchport trunk pvid vlan 100
PE1(config-if-gigabitethernet0/1)#exit
```

#On PE1, configure the link type of port gigabitethernet0/2 as Trunk, and allow services of VLAN15~VLAN30 and VLAN101 to pass. Configure PVID as 1.

```
PE1(config)#interface gigabitethernet 0/2
PE1(config-if-gigabitethernet0/2)#switchport mode trunk
PE1(config-if-gigabitethernet0/2)#switchport trunk allowed vlan add 15-30,101
PE1(config-if-gigabitethernet0/2)#switchport trunk pvid vlan 101
PE1(config-if-gigabitethernet0/2)#exit
```

#On PE1, configure the link type of port gigabitethernet0/3 as Trunk, and allow services of VLAN100 and VLAN101 to pass. Configure PVID as 1.

```
PE1(config)#interface gigabitethernet 0/3
PE1(config-if-gigabitethernet0/3)#switchport mode trunk
PE1(config-if-gigabitethernet0/3)#switchport trunk allowed vlan add 100,101
PE1(config-if-gigabitethernet0/3)#switchport trunk pvid vlan 1
PE1(config-if-gigabitethernet0/3)#exit
```

#Configure flexible QinQ function on the port gigabitethernet0/1 of PE1 so that outer Tag VLAN100 is added to the data of VLAN10~VLAN20.

```
PE1(config)#interface gigabitethernet 0/1
PE1(config-if-gigabitethernet0/1)#vlan dot1q-tunnel 10-20 100
PE1(config-if-gigabitethernet0/1)#exit
```

#Configure QinQ function on the port gigabitethernet0/2 of PE1 so that outer Tag VLAN101 is added to the data of VLAN15~VLAN30.

```
PE1(config)#interface gigabitethernet 0/2
PE1(config-if-gigabitethernet0/2)#vlan dot1q-tunnel 15-30 101
PE1(config-if-gigabitethernet0/2)#exit
```

#View the information of flexible QinQ entry on PE1.

```
PE1#show vlan dot1q-tunnel
-----VLAN DOT1Q-TUNNEL-----
Interface      priority-default  Inner VlanId  Outer VlanId  inner-priority-trust  Inner VlanId Count
-----
gi0/1          disable          10-20        100           /                     11
gi0/2          disable          15-30        101           /                     16
```

**Step 2: Configure PE2.**

#Create VLAN 10~VLAN30 and VLAN100~VLAN101 on PE2.

```
PE2#configure terminal
PE2(config)#vlan 10-30,100-101
```

#On PE2, configure the link type of port gigabitEthernet0/1 as Trunk, and allow services of VLAN10~VLAN20 and VLAN100 to pass. Configure PVID as configured as 1.

```
PE2(config)#interface gigabitEthernet 0/1
PE2(config-if-gigabitEthernet0/1)#switchport mode trunk
PE2(config-if-gigabitEthernet0/1)#switchport trunk allowed vlan add 10-20,100
PE2(config-if-gigabitEthernet0/1)#switchport trunk pvid vlan 100
PE2(config-if-gigabitEthernet0/1)#exit
```

#On PE2, configure the link type of port gigabitEthernet0/2 as Trunk, and allow services of VLAN15~VLAN30 and VLAN101 to pass. Configure PVID as 1.

```
PE2(config)#interface gigabitEthernet 0/2
PE2(config-if-gigabitEthernet0/2)#switchport mode trunk
PE2(config-if-gigabitEthernet0/2)#switchport trunk allowed vlan add 15-30,101
PE2(config-if-gigabitEthernet0/2)#switchport trunk pvid vlan 101
PE2(config-if-gigabitEthernet0/2)#exit
```

#On PE2, configure the link type of port gigabitEthernet0/3 as Trunk, and allow services of VLAN100 and VLAN101 to pass. Configure PVID as 1.

```
PE2(config)#interface gigabitEthernet 0/3
PE2(config-if-gigabitEthernet0/3)#switchport mode trunk
PE2(config-if-gigabitEthernet0/3)#switchport trunk allowed vlan add 100,101
PE2(config-if-gigabitEthernet0/3)#switchport trunk pvid vlan 1
PE2(config-if-gigabitEthernet0/3)#exit
```

#Configure flexible QinQ function on the port gigabitEthernet0/1 of PE2 so that outer Tag VLAN100 is added to the data of VLAN10~VLAN20.

```
PE2(config)#interface gigabitEthernet 0/1
PE2(config-if-gigabitEthernet0/1)#vlan dot1q-tunnel 10-20 100
PE2(config-if-gigabitEthernet0/1)#exit
```

#Configure flexible QinQ function on the port gigabitEthernet0/2 of PE2 so that outer Tag VLAN101 is added to the data of VLAN15~VLAN30.

```
PE2(config)#interface gigabitEthernet 0/2
PE2(config-if-gigabitEthernet0/2)#vlan dot1q-tunnel 15-30 101
PE2(config-if-gigabitEthernet0/2)#exit
```

#View the information of flexible QinQ entry on PE2.

```
PE2#show vlan dot1q-tunnel
-----VLAN DOT1Q-TUNNEL-----
Interface      priority-default  Inner VlanId  Outer VlanId  inner-priority-trust  Inner VlanId Count
-----
gi0/1          disable          10-20        100           /                     11
gi0/2          disable          15-30        101           /                     16
```

Step 3: Check the result.

#Services between intranet users CE1 and CE2 can communicate on the operator's network VLAN100 through PE1 and PE2 with double layers of Tag; those between CE3 and CE4 can communicate on the operator's network VLAN101 through PE1 and PE2 with double layers of Tag.

### 28.3.3 Configure 1:1 VLAN mapping

#### Network Requirements

- Intranet users CE1 and CE2, CE3 and CE4 communicate through the operator's network. CE1 and CE2 use intranet VLAN2, while CE3 and CE4 use intranet VLAN3. PE1 and PE2 are edge devices for the operator's network.
- Configure 1:1 VLAN rules on PE1 and PE2 so that CE1 and CE2, CE3 and CE4 can communicate with each other through the operator's public network VLAN 100 and VLAN101. The data has a single layer of Tag when transmitting on the operator's network.

#### Network Topology

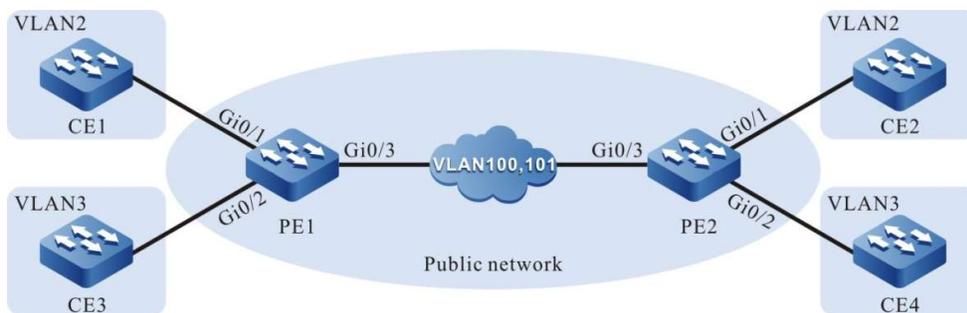


Figure 2 Configuring Network Topology of 1:1 VLAN Mapping

#### Configuration Steps

Step 1: Configure PE1.

#Create VLAN 2~VLAN3 and VLAN100~VLAN101 on PE1.

```
PE1#configure terminal
PE1(config)#vlan 2-3,100-101
```

#On PE1, configure the link type of port gigabitethernet0/1 as Trunk, and allow services of VLAN2 and VLAN100 to pass. Configure PVID as 1.

```
PE1(config)#interface gigabitethernet 0/1
PE1(config-if-gigabitethernet0/1)#switchport mode trunk
PE1(config-if-gigabitethernet0/1)#switchport trunk allowed vlan add 2,100
PE1(config-if-gigabitethernet0/1)#switchport trunk pvid vlan 1
PE1(config-if-gigabitethernet0/1)#exit
```

#On PE1, configure the link type of port gigabitethernet0/2 as Trunk, and allow services of VLAN3 and VLAN101 to pass. Configure PVID as 1.

```
PE1(config)#interface gigabitethernet 0/2
PE1(config-if-gigabitethernet0/2)#switchport mode trunk
PE1(config-if-gigabitethernet0/2)#switchport trunk allowed vlan add 3,101
PE1(config-if-gigabitethernet0/2)#switchport trunk pvid vlan 1
PE1(config-if-gigabitethernet0/2)#exit
```

#On PE1, configure the link type of port gigabitethernet0/3 as Trunk, and allow services of VLAN100 and VLAN101 to pass. Configure PVID as 1.

```
PE1(config)#interface gigabitethernet 0/3
PE1(config-if-gigabitethernet0/3)#switchport mode trunk
PE1(config-if-gigabitethernet0/3)#switchport trunk allowed vlan add 100,101
PE1(config-if-gigabitethernet0/3)#switchport trunk pvid vlan 1
PE1(config-if-gigabitethernet0/3)#exit
```

#Configure 1:1 VLAN mapping function on the port gigabitethernet0/1 of PE1 so that the data of VLAN2 is modified into VLAN100.

```
PE1(config)#interface gigabitethernet 0/1
PE1(config-if-gigabitethernet0/1)#vlan dot1q-tunnel mapping 2 100
PE1(config-if-gigabitethernet0/1)#exit
```

#Configure 1:1 VLAN mapping function on the port gigabitethernet0/2 of PE1 so that the data of VLAN3 is modified into VLAN101.

```
PE1(config)#interface gigabitethernet 0/2

PE1(config-if-gigabitethernet0/2)# vlan dot1q-tunnel mapping 3 101
PE1(config-if-gigabitethernet0/2)#exit
```

#View the information of 1:1 VLAN mapping entry on PE1.

```
PE1#show vlan dot1q-tunnel mapping
-----VLAN DOT1Q-TUNNEL MAPPING-----
Interface      priority-default  Former VlanId  Mapping VlanId  inner-priority-trust  Former VlanId Count
-----
gi0/1          disable          2             100             /                     1
gi0/2          disable          3             101             /                     1
```

## Step 2: Configure PE2.

#Create VLAN 2~VLAN3 and VLAN100~VLAN101 on PE2.

```
PE2#configure terminal
PE2(config)#vlan 2-3,100-101
```

#On PE2, configure the link type of port gigabitethernet0/1 as Trunk, and allow services of VLAN2 and VLAN100 to pass. Configure PVID as 1.

```
PE2(config)#interface gigabitethernet 0/1
PE2(config-if-gigabitethernet0/1)#switchport mode trunk
PE2(config-if-gigabitethernet0/1)#switchport trunk allowed vlan add 2,100
PE2(config-if-gigabitethernet0/1)#switchport trunk pvid vlan 1
PE2(config-if-gigabitethernet0/1)#exit
```

#On PE2, configure the link type of port gigabitethernet0/2 as Trunk, and allow services of VLAN3 and VLAN101 to pass. Configure PVID as 1.

```
PE2(config)#interface gigabitethernet 0/2
PE2(config-if-gigabitethernet0/2)#switchport mode trunk
PE2(config-if-gigabitethernet0/2)#switchport trunk allowed vlan add 3,101
PE2(config-if-gigabitethernet0/2)#switchport trunk pvid vlan 1
PE2(config-if-gigabitethernet0/2)#exit
```

#On PE2, configure the link type of port gigabitethernet0/3 as Trunk, and allow services of VLAN100 and VLAN101 to pass. Configure PVID as 1.

```

PE2(config)#interface gigabitethernet 0/3
PE2(config-if-gigabitethernet0/3)#switchport mode trunk
PE2(config-if-gigabitethernet0/3)#switchport trunk allowed vlan add 100,101
PE2(config-if-gigabitethernet0/3)#switchport trunk pvid vlan 1
PE2(config-if-gigabitethernet0/3)#exit

```

#Configure 1:1 VLAN mapping function on the port gigabitethernet0/1 of PE2 so that the data of VLAN2 is modified into VLAN100.

```

PE2(config)#interface gigabitethernet 0/1
PE2(config-if-gigabitethernet0/1)#vlan dot1q-tunnel mapping 2 100
PE2(config-if-gigabitethernet0/1)#exit

```

#Configure 1:1 VLAN mapping function on the port gigabitethernet0/2 of PE2 so that the data of VLAN3 is modified into VLAN101.

```

PE2(config)#interface gigabitethernet 0/2
PE2(config-if-gigabitethernet0/2)#vlan dot1q-tunnel mapping 3 101
PE2(config-if-gigabitethernet0/2)#exit

```

#View the information of 1:1 VLAN mapping entry on PE2.

```

PE2#show vlan dot1q-tunnel mapping
-----VLAN DOT1Q-TUNNEL MAPPING-----
Interface      priority-default  Former VlanId  Mapping VlanId  inner-priority-trust  Former VlanId Count
-----
gi0/1          disable          2              100             /                    1
gi0/2          disable          3              101             /                    1

```

Step 3: Check the result.

#Services between intranet users CE1 and CE2 can communicate on the operator's network VLAN100 through PE1 and PE2 with a single layer of Tag; those between CE3 and CE4 can communicate on the operator's network VLAN101 through PE1 and PE2 with a single layer of Tag.

### 28.3.4 Configure N: 1 VLAN mapping

#### Network Requirements

- On Device2, in different VLANs, services of PC1 and PC2 are isolated from each other.
- Configure N: 1 VLAN mapping function on Device1 so that the service packets of PC1 and PC2 transmit in the same VLAN when passing through Device1 to save VLAN resource.

#### Network Topology

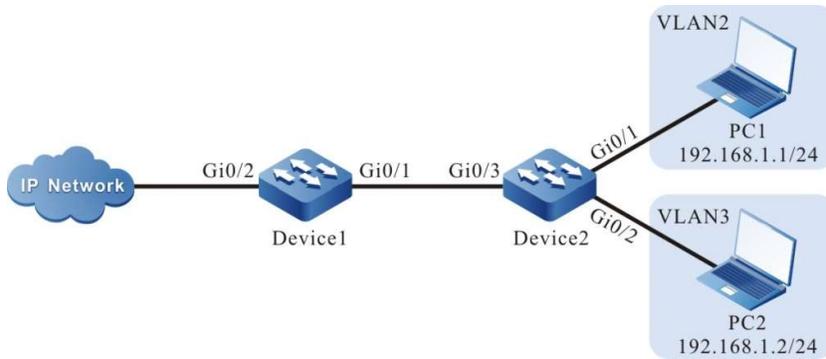


Figure 3 Configuring Network Topology of N:1 VLAN Mapping

### Configuration Steps

Step 1: Configure Device1.

#Create VLAN2~VLAN4 on Device1.

```
Device1#configure terminal
Device1(config)#vlan 2-4
```

#On Device1, configure the link type of port gigabitethernet0/1 as Trunk, and allow services of VLAN2~VLAN4 to pass. Configure PVID as 1.

```
Device1(config)#interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#switchport mode trunk
Device1(config-if-gigabitethernet0/1)#switchport trunk allowed vlan add 2-4
Device1(config-if-gigabitethernet0/1)#switchport trunk pvid vlan 1
```

#Configure N:1 VLAN mapping function on the port gigabitethernet0/1 of Device1 so that the VLAN2 and VLAN3 are mapped to VLAN4.

```
Device1(config-if-gigabitethernet0/1)#vlan dot1q-tunnel mapping n-to-1 enable
Device1(config-if-gigabitethernet0/1)#vlan dot1q-tunnel mapping n-to-1 2-3 4
Device1(config-if-gigabitethernet0/1)#exit
```

#On Device1, configure the link type of port gigabitethernet0/2 as Trunk, and allow services of VLAN2~VLAN4 to pass. Configure PVID as 1.

```
Device1(config)#interface gigabitethernet 0/2
Device1(config-if-gigabitethernet0/2)#switchport mode trunk
Device1(config-if-gigabitethernet0/2)#switchport trunk allowed vlan add 2-4
Device1(config-if-gigabitethernet0/2)#switchport trunk pvid vlan 1
Device1(config-if-gigabitethernet0/2)#exit
```

Step 2: Configure Device2.

#Create VLAN2 and VLAN3 on Device2.

```
Device2#configure terminal
Device2(config)#vlan 2-3
```

#Configure the link type of port gigabitethernet0/1 on Device2 as Access, allowing the services of VLAN2 to pass.

```
Device2(config)#interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#switchport mode access
Device2(config-if-gigabitethernet0/1)#switchport access vlan 2
Device2(config-if-gigabitethernet0/1)#exit
```

#Configure the link type of port gigabitethernet0/2 on Device2 as Access, allowing the services of VLAN3 to pass.

```
Device2(config)#interface gigabitethernet 0/2
Device2(config-if-gigabitethernet0/2)#switchport mode access
Device2(config-if-gigabitethernet0/2)#switchport access vlan 3
Device2(config-if-gigabitethernet0/2)#exit
```

#On Device2, configure the link type of port gigabitethernet0/3 as Trunk, and allow services of VLAN2 and VLAN3 to pass. Configure PVID as 1.

```
Device2(config)#interface gigabitethernet 0/3
Device2(config-if-gigabitethernet0/3)#switchport mode trunk
Device2(config-if-gigabitethernet0/3)#switchport trunk allowed vlan add 2-3
Device2(config-if-gigabitethernet0/3)#switchport trunk pvid vlan 1
Device2(config-if-gigabitethernet0/3)#exit
```

*Step*  
3:

Check the result.

#View the information of N:1 VLAN mapping entry on Device1.

```
Device1#show vlan dot1q-tunnel mapping n-to-1 configuration
-----
NO. Name          Status Customer Member          Service VLAN
-----
1  gi0/1          enable 2-3                4
```

#On Device2, services of PC1 and PC2 are isolated from each other. The service packet of PC1 transmits in VLAN2, and that of PC2 in VLAN3.

#The service packets of PC1 and PC2 that access IP Network are forwarded via the VLAN4 of Device1.

# 29 Super-VLAN

---

## 29.1 Overview

Different VLANs are isolated from each other at layer 2. To enable them to communicate with each other, you must configure a VLAN interface and IP address for each VLAN. However, this mode consumes a large number of scarce IP address resources. Super-VLAN, also called VLAN aggregation, can solve this problem effectively. A common VLAN, after being added into a super-VLAN, becomes a sub-VLAN of the super-VLAN. If the Address Resolution Protocol (ARP)/ND proxy function is enabled for the super-VLAN, the super-VLAN shares its VLAN interface with its sub-VLANs. In this way, the sub-VLANs take the VLAN interface IP/IPv6 address of the super-VLAN as the gateway to implement layer-3 communication. This saves IP address resources.

## 29.2 VLAN Function Configuration

Table 29 Super-VLAN Function Configuration List

Configuration Task	
Configure a super VLAN.	Configure a super VLAN.
Configure sub-VLAN members of the super-VLAN.	Configure sub-VLAN members of the super-VLAN.
Enable the ARP proxy function.	Enable the ARP proxy function.
Enable the ND proxy function.	Enable the ND proxy function.

### 29.2.1 Configure a super VLAN.

#### Configuration Condition

None

User manual  
Release 1.0 01/2022

### Configure a super VLAN.

On the Super-VLAN, VLAN can be configured, but port cannot be added. The Super-VLAN shall not be the existing VLAN or Sub-VLAN.

Table 1 Configuring Super-VLAN

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Create Super-VLAN	<b>super-vlan <i>vlan-id</i></b>	Mandatory  By default, no Super-VLAN is created.  Upon creation of the Super-VLAN, you will enter the Super-VLAN configuration mode automatically.
Configure description for Super-VLAN	<b>description <i>description</i></b>	Optional  By default, Super-VLAN is described as "SuperVLAN <i>vlan-id</i> ", such as "SuperVLAN0100".

### 29.2.2 Configure sub-VLAN members of the super-VLAN.

#### Configuration Condition

None

#### Configure sub-VLAN members of the super-VLAN.

One super-VLAN supports a maximum of 8 sub-VLAN members, and one VLAN can become the sub-VLAN member of only one super-VLAN. On a sub-VLAN, a VLAN interface cannot be configured but a port can be added into it. The method for adding a port into a sub-VLAN is the same as the method for adding a port into a common VLAN. The VLAN ID of a sub-VLAN must not be identical with the VLAN ID of an existing super-VLAN.

Table 29 Configuring Sub-VLAN Members of Super-VLAN

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the super-VLAN configuration mode.	<b>super-vlan <i>vlan-id</i></b>	-
Configure sub-VLAN members of the super-VLAN.	<b>sub-vlan <i>vlan-list</i></b>	Mandatory  By default, a super-VLAN is not configured with sub-VLAN members.

---

### Caution

- If Sub-VLAN has been configured, it cannot be configured as an exclusive EIPS control VLAN.
- 

## 29.2.3 Enable the ARP proxy function.

### Configuration Condition

Before enabling the ARP proxy function, ensure that:

- The VLAN interface corresponding to the super-VLAN and the IP address have been configured.

### Configure the ARP Proxy Function

After the ARP proxy function of a super-VLAN is configured, the sub-VLANs can communicate with each other at layer 3 through ARP proxy.

Table 2 Enabling ARP Proxy Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the super-VLAN configuration mode.	<b>super-vlan <i>vlan-id</i></b>	-
Enable the ARP proxy function.	<b>arp proxy enable</b>	Mandatory

Step	Command	Description
		By default, the ARP proxy function is disabled.

### Note

- The ARP proxy function relies on the layer-3 forwarding function. If the device does not support the layer-3 forwarding function, the ARP proxy function does not take effect.

## 29.2.4 Enable the ND proxy function.

### Configuration Condition

Before enabling the ND proxy function, ensure that:

- The VLAN interface corresponding to the super-VLAN and the IPv6 address have been configured.

### Configure the ND Proxy Function

After the ND proxy function of a super-VLAN is configured, the sub-VLANs can communicate with each other at IPv6 layer 3 through ND proxy.

Table 3 Enabling ND Proxy Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the super-VLAN configuration mode.	<b>super-vlan <i>vlan-id</i></b>	-
Enable the ND proxy function.	<b>nd local-proxy enable</b>	Mandatory By default, the ND proxy function is disabled.

### Note

- The ND proxy function relies on the layer 3 forwarding function. If the device does not support the IPv6 layer 3 forwarding function, the ND proxy function does not take effect.

## 29.2.5 VLAN Monitoring and Maintaining

Table 4 Super-VLAN Monitoring and Maintaining

Command	Description
<b>show super-vlan [ <i>vlan-id</i> ]</b>	Displays the information about the specified super-VLAN.
<b>show super-vlan config { <i>vlan-id</i>   all }</b>	Show Super-VLAN configuration information
<b>show super-vlan [ <i>vlan-id</i> ] portlist</b>	Show the information of port under the management of Super-VLAN
<b>show super-vlan <i>vlan-id</i> sub-vlan <i>vlan-id</i> portlist</b>	Show the information of port under the management of Sub-VLAN

## 29.3 Super-VLAN Typical Configuration Example

### 29.3.1 Configure a super VLAN.

#### Network Requirements

- PC1 and PC2 are two hosts in Sub-VLAN2, PC3 is a host in Sub-VLAN3, and Server is a server in VLAN5.
- The super-VLAN function has been configured on Device. Then, PC1 and PC2 can intercommunicate with each other at layer2. PC1 and PC2 can intercommunicate with PC3 at layer3, and they can access the server.

#### Network Topology

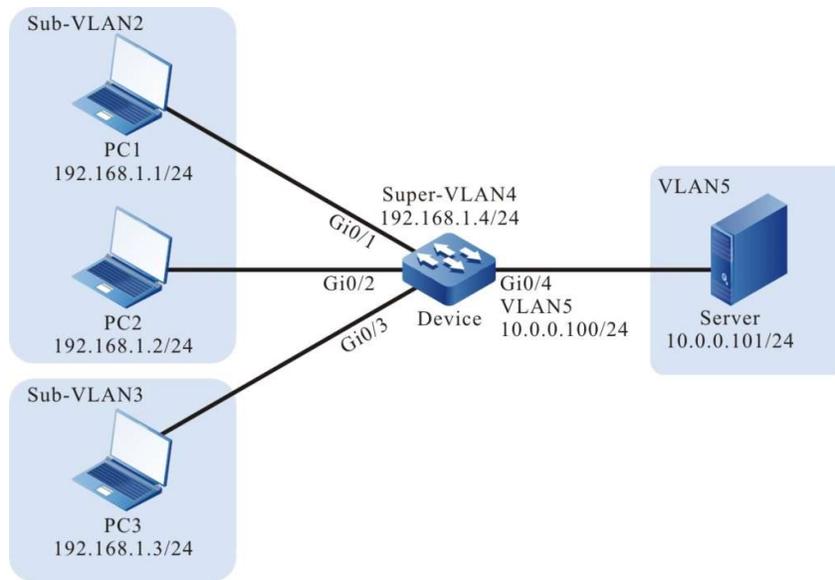


Figure 29 Network Topology for Configuration of Super-VLAN

### Configuration Steps

Step 1: Configure VLAN and port link type on Device.

#Create VLAN2, VLAN3 and VLAN5 on Device.

```
Device#configure terminal
Device(config)#vlan 2-3,5
```

#On the Device, configure the IP address of VLAN interface 4 as 192.168.1.4 and mask as 255.255.255.0; configure the IP address of VLAN interface 5 as 10.0.0.100 and mask as 255.255.255.0.

```
Device(config)#interface vlan 4
Device(config-if-vlan4)#ip address 192.168.1.4 255.255.255.0
Device(config-if-vlan4)#exit
Device(config)#interface vlan 5
Device(config-if-vlan5)#ip address 10.0.0.100 255.255.255.0
Device(config-if-vlan5)#exit
```

#Configure the link type of port gigabitethernet0/1~gigabitethernet0/2 on the Device as Access, allowing the services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/1,0/2
Device(config-if-range)#switchport mode access
Device(config-if-range)#switchport access vlan 2
Device(config-if-range)#exit
```

#Configure the link type of port gigabitethernet0/3 on the Device as Access, allowing the services of VLAN3 to pass.

```
Device(config)#interface gigabitethernet 0/3
Device(config-if-gigabitethernet0/3)#switchport mode access
Device(config-if-gigabitethernet0/3)#switchport access vlan 3
Device(config-if-gigabitethernet0/3)#exit
```

#Configure the link type of port gigabitethernet0/4 on the Device as Access, allowing the services of VLAN5 to pass.

```

Device(config)#interface gigabitethernet 0/4
Device(config-if-gigabitethernet0/4)#switchport mode access
Device(config-if-gigabitethernet0/4)#switchport access vlan 5
Device(config-if-gigabitethernet0/4)#exit

```

#View the information of VLAN and port of the Device.

```

Device#show vlan 2
-----
NO. VID VLAN-Name      Owner Mode  Interface
-----
1 2  VLAN0002          static Untagged gi0/1 gi0/2
Device#show vlan 3
-----
NO. VID VLAN-Name      Owner Mode  Interface
-----
1 3  VLAN0003          static Untagged gi0/3
Device#show vlan 5
-----
NO. VID VLAN-Name      Owner Mode  Interface
-----
1 5  VLAN0005          static Untagged gi0/4

```

Step 2: Configure the Super-VLAN function on the Device.

#On the Device, configure VLAN4 as Super-VLAN, VLAN2 and VLAN3 as Sub-VLAN, and enable ARP proxy.

```

Device(config)#super-vlan 4
Device(config-super-vlan4)#sub-vlan 2,3
Device(config-super-vlan4)#arp proxy enable
Device(config-super-vlan4)#exit

```

#View the information of Super-VLAN on the Device.

```

Device#show super-vlan
-----
NO. SuperVlan Description      Arp Proxy SubVlan Member
-----
1 4      SuperVLAN0004          enable    2-3

```

---

## Caution

- To achieve intercommunication between hosts in different Sub-VLANs at layer 3, the ARP proxy function must be enabled.
  - Super-VLAN and Sub-VLAN must be in the same spanning tree instance.
- 

Step 3: Check the result. Use the ping command to check the connectivity between PC1, PC2, PC3 and the server.

#PC1 and PC2 in Sub-VLAN2 can ping each other successfully.

#PC1 and PC2 in Sub-VLAN2 and PC3 in Sub-VLAN3 can ping each other successfully.

#PC1, PC2, and PC3 in Sub-VLANs and the server can ping each other successfully.



# 30 PVLAN

---

## 30.1 Overview

In order to isolate all users from each other and allow them to access common resources, usually each user need to be provided with a VLAN. However, for the application scenarios with many users, since there are only 4,094 VLANs in total, when the number of users exceeds this figure, the number of VLANs will become a bottleneck and make it difficult to conduct configuration, management and maintenance. To cope with this problem, PVLAN (Private VLAN) is born. Through a flexible VLAN configuration mode, it can effectively configure and utilize VLAN and IP address resources, and simplify network configuration.

PVLAN employs a two-layer VLAN structure, i.e. Primary VLAN and Secondary VLAN. Generally, Primary VLAN connects with uplink device, and Secondary VLAN with downlink device. According to the forwarding rules of layer 2, Secondary VLANs are divided into the following two types:

- **Isolated VLAN:** Member ports, whether within the same Isolated VLAN or not, are isolated from each other at layer 2. Users can be isolated from each other only if the ports connecting users are added to the Isolated VLAN;
- **Community VLAN:** The forwarding rules of Community VLAN are the same as those of common VLAN. Member ports in the same Community VLAN can communicate with each other at layer 2, and stay isolated from those of other Community VLAN and Isolated VLAN.

After Primary VLAN and Secondary VLAN are associated with each other, the member ports in Secondary VLAN can directly communicate with those in Primary VLAN at layer 2, and with the outside through the VLAN interface on Primary VLAN at layer 3.

PVLAN has two specific port link types, i.e. Promiscuous and Host. Promiscuous port can only be added to Primary VLAN, and Host port can only be added to Secondary VLAN. The Host port added to the Community VLAN is also called Community port, and the Host port added to the Isolated VLAN is also called Isolated port.

## 30.2 PVLAN function configuration

Table 30 PVLAN Function Configuration List

Configuration Task	
Configure Primary VLAN	Configure Primary VLAN
Add ports into Primary VLAN	Add ports into Primary VLAN
Configure Secondary VLAN	Configure Secondary VLAN
Add ports into Secondary VLAN	Add ports into Secondary VLAN
Configure the association relationship between Primary VLAN and Secondary VLAN	Configure the association relationship between Primary VLAN and Secondary VLAN

### 30.2.1 Configure Primary VLAN

The uplink device recognizes Primary VLAN only. It never cares about its associated Secondary VLAN.

#### Configuration Condition

None

#### Configure Primary VLAN

Table 30 Configuring Primary VLAN

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the VLAN configuration mode	<b>vlan <i>vlan-id</i></b>	-
Configure the VLAN type as Primary VLAN	<b>private-vlan primary</b>	Mandatory By default, all VLANs are common.

## 30.2.2 Add ports into Primary VLAN

Only the ports with link type being Promiscuous can be added into Primary VLAN. The ports added into Primary VLAN can communicate with other member ports in Primary VLAN and the member ports in Secondary VLAN associated with this Primary VLAN at layer 2. Generally, Promiscuous ports are used as uplink ports.

### Configuration Condition

Before adding ports into Primary VLAN, the following tasks should be completed:

- Configure the type of VLAN where ports are added as Primary VLAN.

### Add ports into Primary VLAN

Table 1 Add Ports into Primary VLAN

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Configure the port link type as Promiscuous	<b>switchport mode private-vlan promiscuous</b>	Mandatory By default, the port link type is the Access type.
Add Promiscuous ports into Primary VLAN	<b>private-vlan promiscuous</b> <i>vlan-id</i>	Mandatory By default, Promiscuous ports are not added into any VLAN.

---

## Note

- If the port is not added into Primary VLAN when the port link type is configured as Promiscuous, the PVLAN function of the port will not take effect, and the Promiscuous port will be exclusive for PVLAN, which means other functions cannot be applied to the Promiscuous port. Therefore, it is recommended to complete the configuration as per the steps mentioned above.
- 

### 30.2.3 Configure Secondary VLAN

The downlink device recognizes Primary VLAN only. It never cares about its associated Primary VLAN.

#### Configuration Condition

None

#### Configure Secondary VLAN

Table 2 Configuring Secondary VLAN

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the VLAN configuration mode	<b>vlan <i>vlan-id</i></b>	-
Configure the VLAN type as Secondary VLAN	<b>private-vlan { community   isolated }</b>	Mandatory By default, all VLANs are common.

### 30.2.4 Add ports into Secondary VLAN

Only the ports with the link type being Host can be added into Secondary VLAN which has two types: Community VLAN and Isolated VLAN. The ports added into Community VLAN can only communicate with other member ports in this Community VLAN and the member ports in the Primary VLAN associated with this Community VLAN at layer 2. The ports added into Isolated VLAN can only communicate with the member ports in the Primary VLAN associated with this Isolated VLAN at layer 2. Generally, Host ports are used as downlink ports.

#### Configuration Condition

Before adding ports into Secondary VLAN, the following tasks should be completed:

- Configure the type of VLAN where ports are added as Secondary VLAN.

### Add ports into Secondary VLAN

Table 3 Add Ports into Secondary VLAN

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	At least one option must be selected.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	After you enter the interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Configure the port link type as Host.	<b>switchport mode private-vlan host</b>	Mandatory By default, the link type is Access.
Add Host ports into Secondary VLAN	<b>private-vlan host</b> <i>vlan-id</i>	Mandatory By default, Host ports are not added into any VLAN.

### Note

- The host in Secondary VLAN cannot communicate with the VLAN interface of this device at layer 3.
- If the port is not added into Primary VLAN when the port link type is configured as Host, the PVLAN function of the port will not take effect, and the Host port will be exclusive for PVLAN, which means other functions cannot be applied to the Host port. Therefore, it is recommended to complete the configuration as per the steps mentioned above.

### 30.2.5 Configure the association relationship between Primary VLAN and Secondary VLAN

After association is established, the hosts in Primary VLAN can communicate with those in the associated Secondary VLAN at layer 2. One Primary VLAN can associate with one Isolated VLAN at most and 192 Community VLANs. One Secondary VLAN can associate with one Primary VLAN only.

#### Configuration Condition

Before associating Primary VLAN with Secondary VLAN, the following tasks should be completed:

- Configure the type of VLAN in current VLAN configuration mode as Primary VLAN.

#### Configure the association relationship between Primary VLAN and Secondary VLAN

Table 4 Configuring Association Relationship Between Primary VLAN and Secondary VLAN

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the VLAN configuration mode	<b>vlan <i>vlan-id</i></b>	-
Configure the association relationship of Primary VLAN	<b>private-vlan association add <i>vlan-list</i></b>	Mandatory  By default, Primary VLAN doesn't associate with any Secondary VLAN.

---

#### Note

- If the Primary VLAN associates with a common VLAN, the association will not take effect unless the type of common VLAN is changed to Secondary VLAN.
  - If Secondary VLAN is associated with Primary VLAN, then for the MAC address entry dynamically learned through Secondary VLAN, the VLAN recorded in FDB table is the Primary VLAN associated with this Secondary VLAN rather than the Secondary VLAN itself.
- 

### 30.2.6 PVLAN Monitoring and Maintaining

Table 5 PVLAN Monitoring and Maintaining

Command	Description
<b>show private-vlan [ vlan-id ]</b>	Show PVLAN information

## 30.3 Typical PVLAN Configuration Example

### 30.3.1 Configure PVLAN

#### Network Requirements

- PC1 and PC2 belong to Secondary VLAN2; PC3 and PC4 belong to Secondary VLAN3; Server belongs to Primary VLAN4.
- Configure PVLAN on the Device for intercommunication in Secondary VLAN2, mutual isolation in Secondary VLAN3, isolation between Secondary VLAN2 and Secondary VLAN3, and intercommunication of both Secondary VLAN2 and Secondary VLAN3 with Primary VLAN4.

#### Network Topology

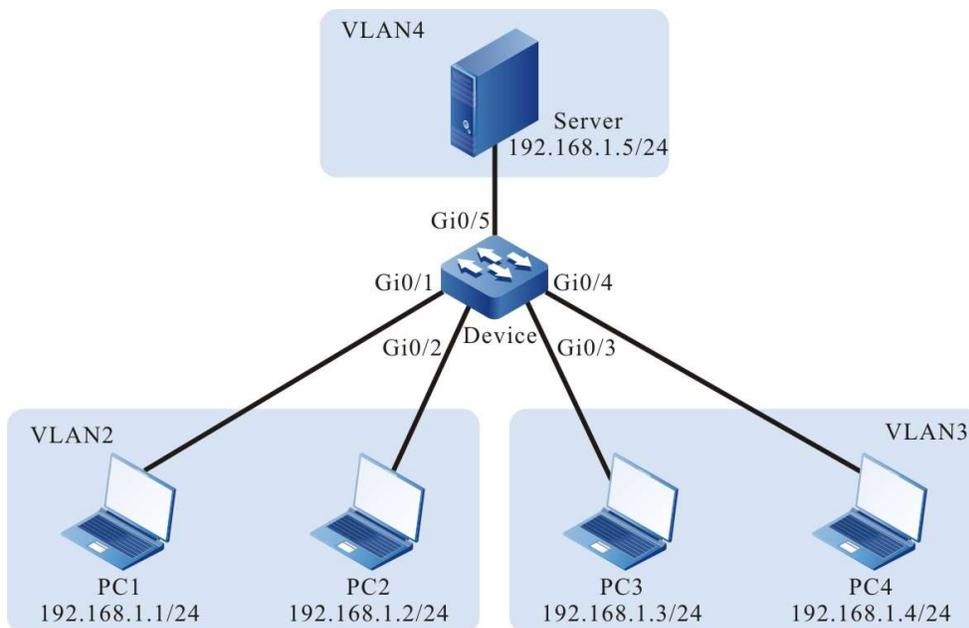


Figure 30 Network Topology for Configuration of PVLAN

#### Configuration Steps

*Step 1:* Configure VLAN on the Device.

#Create VLAN2~VLAN4 on the Device.

```
Device#configure terminal
Device(config)#vlan 2-4
```

*Step*  
*2:* Configure the PVLAN function on the Device.

#On the Device, configure VLAN4 as Primary VLAN, VLAN2 as Community VLAN, and VLAN3 as Isolated VLAN.

```
Device(config)#vlan 4
Device(config-vlan4)#private-vlan primary
Device(config-vlan4)#vlan 2
Device(config-vlan2)#private-vlan community
Device(config-vlan2)#vlan 3
Device(config-vlan3)#private-vlan isolated
Device(config-vlan3)#exit
```

#Associate Primary VLAN4 with Community VLAN2 and Isolated VLAN3 on the Device.

```
Device(config)#vlan 4
Device(config-vlan4)#private-vlan association add 2,3
Device(config-vlan4)#exit
```

#Configure the link type of port gigabitethernet0/1~gigabitethernet0/2 on the Device as Host, and add them into VLAN2.

```
Device(config)#interface gigabitethernet 0/1-0/2
Device(config-if-range)#switchport mode private-vlan host
Device(config-if-range)#private-vlan host 2
Device(config-if-range)#exit
```

#Configure the link type of port gigabitethernet0/3~gigabitethernet0/4 on the Device as Host, and add them into VLAN3.

```
Device(config)#interface gigabitethernet 0/3-0/4
Device(config-if-range)#switchport mode private-vlan host
Device(config-if-range)#private-vlan host 3
Device(config-if-range)#exit
```

#Configure the link type of port gigabitethernet0/5 on the Device as Promiscuous, and add it into VLAN4.

```
Device(config)#interface gigabitethernet 0/5
Device(config-if-gigabitethernet0/5)#switchport mode private-vlan promiscuous
Device(config-if-gigabitethernet0/5)#private-vlan promiscuous 4
Device(config-if-gigabitethernet0/5)#exit
```

*Step*  
*3:* Check the result.

#View the information of PVLAN on the Device.

```
Device#show private-vlan
-----
NO. Primary Secondary Type Interface(Primary) Interface(Secondary)
-----
1 4 3 isolated gi0/5 gi0/3 gi0/4
2 4 2 community gi0/5 gi0/1 gi0/2
```

#The two hosts PC1 and PC2 in Community VLAN2 can ping each other successfully.

#The two hosts PC3 and PC4 in Isolated VLAN3 cannot ping each other successfully.

#The two hosts PC1 and PC2 in Community VLAN2 cannot ping PC3 and PC4 in Isolated VLAN3 successfully.

#Both PC1 and PC2 in Community VLAN2 can ping the Server successfully.

#Both PC3 and PC4 in Isolated VLAN3 can ping the Server successfully.

# 31 Voice-VLAN

## 31.1 Overview

Voice-VLAN is a mechanism that provides security and Quality of Service (QoS) guarantee for voice data flows. In a network, usually two types of traffic coexists, voice data and service data. During transmission, voice data has a higher priority than service data so as to reduce delay and packet loss that may occur during the transmission process. Voice-VLAN can automatically recognize voice traffic and distribute the voice traffic to a specific VLAN with QoS guarantee.

## 31.2 Voice-VLAN Function Configuration

Table 31 Voice-VLAN Function Configuration List

Configuration Task	
Configure a Voice-VLAN	Configure a Voice-VLAN
Configure an OUI Address	Configure an OUI Address
Enable the Voice-VLAN Function of a Port	Enable the Voice-VLAN Function of a Port
Configure the Voice-VLAN Working Mode on the Port	Configure a Voice-VLAN to Automatic Mode
	Configure a Voice-VLAN to Manual Mode
Enable the security mode of Voice-VLAN	Enable the security mode of Voice-VLAN
Enable the Ildp-med authentication mode of Voice-VLAN	Enable the Ildp-med authentication mode of Voice-VLAN

### 31.2.1 Configure a Voice-VLAN

A voice VLAN is used to transmit voice packets. The 802.1p priorities of the recognized voice packets are replaced with the priority of the voice-VLAN. Then the packets are distributed into the voice VLAN for forwarding. A device supports a maximum of one voice-VLAN.

#### Configuration Condition

Before configuring Voice-VLAN, the following tasks should be completed:

- Create the VLAN specified as Voice-VLAN.

#### Configure a Voice-VLAN

Table 31 Configuring Voice-VLAN

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Specify a VLAN as Voice-VLAN	<b>voice vlan <i>vlan-id</i> <i>cos</i> <i>priority</i></b>	Mandatory  By default, Voice-VLAN is not configured, i.e. the Voice-VLAN function is not enabled globally.

### 31.2.2 Configure an OUI Address

#### Configuration Condition

Before configuring an OUI address, ensure that:

- The voice-VLAN function is globally enabled.
- The voice-VLAN function is enabled on the port.

#### Configure an OUI Address

Organizationally Unique Identifiers (OUIs) are used to identify voice packets that are sent by voice devices of manufacturers. After a port that works in voice-VLAN automatic mode receives an Untag packet, it takes out the MAC address of the packet and performs the AND operation with the OUI mask. If the obtained address range is the same as the OUI address, it indicates that matching the OUI address succeeds, and the packet is recognized as a voice packet.

Table 1 Configuring OUI Address

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure an OUI Address	<b>voice vlan oui-mac</b> <i>oui-mac-address</i> <b>mask</b> <i>mask</i> <b>name</b> <i>oui-name</i>	Mandatory  By default, there are 5 default OUI addresses.  The device can support 32 OUI addresses at most.

### 31.2.3 Enable the Voice-VLAN Function of a Port

After the voice-VLAN function is enabled on a port, the port uses a method according to the voice-VLAN working mode to automatically recognize the received packets.

#### Configuration Condition

Before enabling the voice-VLAN function of a port, ensure that:

- The voice-VLAN function is globally enabled.
- The port has been added into the voice-VLAN.

#### Enable the Voice-VLAN Function of a Port

Table 31 Enabling Voice-VLAN Function of Port

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2 Ethernet interface
Enter Aggregation Group Configuration Mode	<b>link-aggregation</b> <i>link-aggregation-id</i>	configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect

Step	Command	Description
		only within the aggregation group.
Enable the Voice-VLAN Function of a Port	<b>voice vlan enable</b>	Mandatory  By default, the port doesn't enable the Voice-VLAN function.

### Note

- The security mode of Voice-VLAN does not support aggregation group. That is to say, when the device enables the security mode of Voice-VLAN, the aggregation group cannot enable the Voice-VLAN function; or when an aggregation group of the device enables the Voice-VLAN function, the security mode of Voice-VLAN cannot be enabled.
- The lldp-med authentication mode of Voice-VLAN does not support aggregation group. That is to say, when the device enables the lldp-med authentication mode of Voice-VLAN, the aggregation group cannot enable the Voice-VLAN function; or when an aggregation group of the device enables the Voice-VLAN function, the lldp-med authentication mode of Voice-VLAN cannot be enabled.

## 31.2.4 Configure the Voice-VLAN Working Mode on the Port

The voice-VLAN of a port can work in automatic mode or manual mode. The ports working in different voice-VLAN modes recognize voice packets in different ways.

- Automatic mode: If the packets received by the port are Untag packets and the source MAC address of the packets matches an OUI address, the packets are regarded as voice packets.
- Manual mode: If the packets received by the port are Untag packets, or Tag packets with the VLAN ID being the port PVID, the packets are regarded as voice packets.

### Configuration Condition

Before configuring the voice-VLAN working mode of a port, ensure that:

- The voice-VLAN function is globally enabled.
- The voice-VLAN function of the port has been enabled.

### Configure a Voice-VLAN to Automatic Mode

Table 2 Configuring Automatic Mode of Voice-VLAN

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>link-aggregation</b> <i>link-aggregation-id</i>	
Make the port work under the automatic mode of Voice-VLAN	<b>voice vlan mode auto</b>	Mandatory  By default, the port works under the automatic mode of Voice-VLAN.

### Configure a Voice-VLAN to Manual Mode

Table 3 Configuring Manual Mode of Voice-VLAN

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode,
Enter Aggregation Group Configuration Mode	<b>link-aggregation</b> <i>link-aggregation-id</i>	

Step	Command	Description
		the subsequent configuration takes effect only within the aggregation group.
Make the port work under the manual mode of Voice-VLAN	<b>no voice vlan mode auto</b>	Mandatory  By default, the port works under the automatic mode of Voice-VLAN.

### Note

- If the port is used to transmit Tagged voice data, the port type should be configured as Trunk or Hybrid only, and the PVID shall not be Voice-VLAN.
- If the port under the manual mode of Voice-VLAN is used to transmit untagged voice data, the PVID must be Voice-VLAN.
- The lldp-med authentication mode of Voice-VLAN does not support manual mode of the port. That is to say, when the device enables the lldp-med authentication mode of Voice-VLAN, the port cannot be configured as the manual mode of Voice-VLAN; or when an port is configured as the manual mode of Voice-VLAN, the lldp-med authentication mode of Voice-VLAN cannot be enabled.

## 31.2.5 Enable the security mode of Voice-VLAN

After the Voice-VLAN security mode is enabled, the device will perform source MAC address matching check on each packet that will enter Voice-VLAN for transmission, and discard those that fail to match the OUI address.

### Configuration Condition

Before enabling the security mode of voice-VLAN, the following tasks should be completed:

- The voice-VLAN function is globally enabled.

### Enable the security mode of Voice-VLAN

Table 4 Enabling Security Mode of Voice-VLAN

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Enable the security mode of Voice-VLAN	<b>voice vlan security enable</b>	Mandatory  By default, the security mode of Voice-VLAN is disabled.

---

### Note

- The security mode of Voice-VLAN does not support aggregation group. That is to say, when the aggregation group of the device enables the function of Voice-VLAN, the security mode of Voice-VLAN cannot be enabled; or when the device enables the security mode of Voice-VLAN, the aggregation group cannot enable the function of Voice-VLAN.
- 

## 31.2.6 Enable the lldp-med authentication mode of Voice-VLAN

After the lldp-med authentication mode of Voice-VLAN is enabled, the device deems the OUI configured by the user or the default OUI as an authentication whitelist, and performs matching check on the source MAC address of the voice device advertised by lldp-med. Only the voice packet sent from the voice device which matches the whitelist can enter the Voice-VLAN for transmission.

### Configuration Condition

Before enabling the lldp-med authentication mode of Voice-VLAN, the following tasks should be completed:

- The voice-VLAN function is globally enabled.

### Enable the lldp-med authentication mode of Voice-VLAN

Table 5 Enabling lldp-med Authentication Mode of Voice-VLAN

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable the lldp-med authentication mode of Voice-VLAN	<b>voice vlan lldp-med authentication</b>	Mandatory  By default, the lldp-med authentication mode of Voice-VLAN is disabled.

---

## Note

- The lldp-med authentication mode of Voice-VLAN does not support aggregation group. That is to say, when the aggregation group of the device enables the function of Voice-VLAN, the lldp-med authentication mode of Voice-VLAN cannot be enabled; or when the device enables the lldp-med authentication mode of Voice-VLAN, the aggregation group cannot enable the function of Voice-VLAN.
  - The lldp-med authentication mode of Voice-VLAN does not support manual mode of the port. That is to say, when any port is configured as the manual mode of Voice-VLAN, the lldp-med authentication mode of Voice-VLAN cannot be enabled; or when the device enables the lldp-med authentication mode of Voice-VLAN, the port cannot be configured as the manual mode of Voice-VLAN.
  - After the lldp-med authentication mode of Voice-VLAN is enabled, the telephone which doesn't support lldp cannot work under normal conditions.
- 

### 31.2.7 Voice-VLAN Monitoring and Maintaining

Table 31 Voice-VLAN Monitoring and Maintaining

Command	Description
<b>show voice vlan { all   interface [ interface-name ]   link-aggregation [ link-aggregation-id ]   oui   lldp-med authenticated-mac }</b>	Show the information of Voice-VLAN

## 31.3 Voice-VLAN Typical Configuration Example

### 31.3.1 Configure a Voice-VLAN to Manual Mode

#### Network Requirements

- IP Phone and PC can access IP Network through Device.
- The voice-VLAN in manual mode has been configured on Device. If the network is normal, IP Phone and PC can normally access IP Network. If the network is congested, IP Phone has a higher priority than PC in accessing IP Network.

#### Network Topology

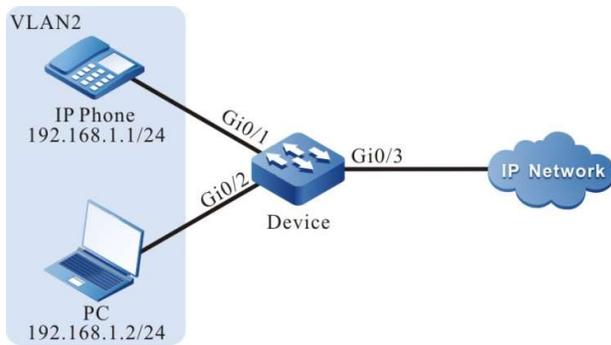


Figure 7-1 Configuration of Network Topology for Manual Mode of Voice-VLAN

### Configuration Steps

*Step 1:* Configure the link type of VLAN and port.

# Create VLAN2 on Device.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the link type of port gigabitethernet0/1 and gigabitethernet0/2 on Device as Access, permitting the services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/1,0/2
Device(config-if-range)#switchport mode access
Device(config-if-range)#switchport access vlan 2
Device(config-if-range)#exit
```

#Configure the link type of port gigabitethernet0/3 on the Device as Trunk, allowing the services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/3
Device(config-if-gigabitethernet0/3)#switchport mode trunk
Device(config-if-gigabitethernet0/3)#switchport trunk allowed vlan add 2
Device(config-if-gigabitethernet0/3)#exit
```

*Step 2:* Configure Voice-VLAN function.

#Configure VLAN2 as Voice-VLAN on the Device, with the value of Cos being 7.

```
Device(config)#voice vlan 2 cos 7
```

#Configure the manual mode of Voice-VLAN on the port gigabitethernet0/1 of the Device.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#voice vlan enable
Device(config-if-gigabitethernet0/1)#no voice vlan mode auto
Device(config-if-gigabitethernet0/1)#exit
```

#View the information of Voice-VLAN on the Device.

```
Device#show voice vlan all
Voice Vlan Global Information: Voice Vlan enable
Voice Vlan security: disable
```

```
Voice Vlan lldp-med authentication: disable
Voice Vlan VID: 2, Cos: 7
Default OUI number: 5
User config OUI number: 0
```

```
Voice vlan interface information:
Interface      Mode
-----
gi0/1         Manual-Mode
```

```
Voice Vlan OUI information: Total: 5
MacAddr      Mask      Name
-----
0003.6b00.0000 ffff.ff00.0000 Cisco-phone default
006b.e200.0000 ffff.ff00.0000 H3C-Aolynk-phone default
00d0.1e00.0000 ffff.ff00.0000 Pingtel-phone default
00e0.7500.0000 ffff.ff00.0000 Polycom-phone default
00e0.bb00.0000 ffff.ff00.0000 3Com-phone default
```

Step 3: Check the result.

#The 802.1p priority of the packets that are sent to IP Phone is modified to 7, and the 802.1p priority of the packets sent by PC to IP Network is not modified.

#When the network is normal, IP Phone and PC can normally access IP Network.

#If the network is congested, IP Phone can access IP Network with a priority higher than PC.

### 31.3.2 Configure a Voice-VLAN to Automatic Mode

#### Network Requirements

- IP Phone and PC access IP Network through port gigabitethernet0/1 of Device. The MAC address of IP Phone is 0001.0001.0001, and the MAC address of PC is 0002.0002.0002.
- The voice-VLAN in automatic mode has been configured. In this way, if the network is normal, IP Phone and PC can normally access IP network. If the network is congested, IP Phone has a higher priority than PC in accessing IP Network.

#### Network Topology

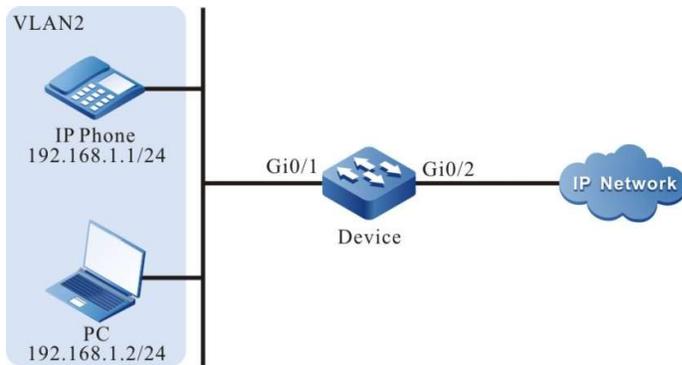


Figure 1 Configuration of Network Topology for Automatic Mode of Voice-VLAN

### Configuration Steps

Step 1: Configure the link type of VLAN and port.

# Create VLAN2 on Device.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the link type of ports gigabitethernet0/1 on the Device as Trunk, allowing the services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)# switchport mode trunk
Device(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2
Device(config-if-gigabitethernet0/1)#exit
```

#Configure the link type of port gigabitethernet0/2 on the Device as Trunk, allowing the services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode trunk
Device(config-if-gigabitethernet0/2)#switchport trunk allowed vlan add 2
Device(config-if-gigabitethernet0/2)#exit
```

Step 2: Configure Voice-VLAN function.

#Configure VLAN2 as Voice-VLAN on the Device, and change corresponding value of Cos to 7.

```
Device(config)#voice vlan 2 cos 7
```

#Configure the automatic mode of Voice-VLAN on the port gigabitethernet0/1 of the Device.

```
Device(config)# interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#voice vlan enable
Device(config-if-gigabitethernet0/1)#voice vlan mode auto
```

```
Device(config-if-gigabitethernet0/1)#exit
```

#Configure the OUI address which corresponds to the MAC address 0001.0001.0001 of IP Phone on the Device.

```
Device(config)#voice vlan oui-mac 0001.0001.0001 mask ffff.ffff.0000 name voice-vlan
```

#View the information of Voice-VLAN on the Device.

```
Device#show voice vlan all
Voice Vlan Global Information: Voice Vlan enable
Voice Vlan security: disable
Voice Vlan lldp-med authentication: disable
Voice Vlan VID: 2, Cos: 7
Default OUI number: 5
User config OUI number: 1

Voice vlan interface information:
Interface      Mode
-----
gi0/1         Auto-Mode

Voice Vlan OUI information: Total: 6
MacAddr      Mask      Name
-----
0001.0001.0000 ffff.ffff.0000 voice-vlan
0003.6b00.0000 ffff.ff00.0000 Cisco-phone default
006b.e200.0000 ffff.ff00.0000 H3C-Aolynk-phone default
00d0.1e00.0000 ffff.ff00.0000 Pingtel-phone default
00e0.7500.0000 ffff.ff00.0000 Polycom-phone default
00e0.bb00.0000 ffff.ff00.0000 3Com-phone default
```

Step 3: Check the result.

#The 802.1 priority of the packets that are sent to IP Phone is modified to 7, and the 802.1P priority of the packets sent by PC to IP Network is not modified.

#When the network is normal, IP Phone and PC can normally access IP Network.

#If the network is congested, IP Phone can access IP Network with a priority higher than PC.

### 31.3.3 Configure the security mode of Voice-VLAN

#### Network Requirements

- IP Phone and PC access IP Network through port gigabitethernet0/1 of Device. The MAC address of IP Phone is 0001.0001.0001, and the MAC address of PC is 0002.0002.0002.
- Configure the security mode of Voice-VLAN on the Device so that IP Phone rather than PC can normally access IP Network.

#### Network Topology

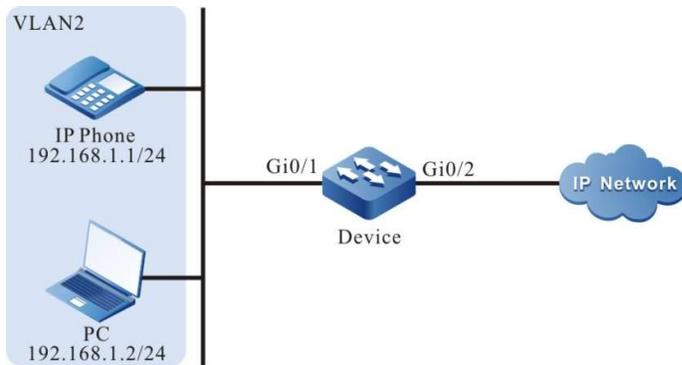


Figure 2 Configuration of Network Topology for Security Mode of Voice-VLAN

### Configuration Steps

Step 1: Configure the link type of VLAN and port.

# Create VLAN2 on Device.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the link type of port gigabitethernet0/1 on the Device as Trunk, allowing the services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode trunk
Device(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2
Device(config-if-gigabitethernet0/1)#exit
```

#Configure the link type of port gigabitethernet0/2 on the Device as Trunk, allowing the services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode trunk
Device(config-if-gigabitethernet0/2)#switchport trunk allowed vlan add 2
Device(config-if-gigabitethernet0/2)#exit
```

Step 2: Configure Voice-VLAN function.

#Configure VLAN2 as Voice-VLAN on the Device, and change corresponding value of Cos to 7.

```
Device(config)#voice vlan 2 cos 7
```

#Globally enable the security mode of Voice-VLAN on the Device.

```
Device(config)# voice vlan security enable
```

#Configure the automatic mode of Voice-VLAN on the port gigabitethernet0/1 of the Device.

```
Device(config)# interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#voice vlan enable
Device(config-if-gigabitethernet0/1)#voice vlan mode auto
Device(config-if-gigabitethernet0/1)#exit
```

#Configure the OUI address which corresponds to the MAC address 0001.0001.0001 of IP Phone on the Device.

```
Device(config)#voice vlan oui-mac 0001.0001.0001 mask ffff.ffff.0000 name voice-vlan
```

#View the information of Voice-VLAN on the Device.

```
Device#show voice vlan all
Voice Vlan Global Information: Voice Vlan enable
Voice Vlan security: enable
Voice Vlan lldp-med authentication: disable
Voice Vlan VID: 2, Cos: 7
Default OUI number: 5
User config OUI number: 1

Voice vlan interface information:
Interface      Mode
-----
gi0/1         Auto-Mode

Voice Vlan OUI information: Total: 6
MacAddr      Mask      Name
-----
0001.0001.0000 ffff.ffff.0000 voice-vlan
0003.6b00.0000 ffff.ff00.0000 Cisco-phone default
006b.e200.0000 ffff.ff00.0000 H3C-Aolynk-phone default
00d0.1e00.0000 ffff.ff00.0000 Pingtel-phone default
00e0.7500.0000 ffff.ff00.0000 Polycom-phone default
00e0.bb00.0000 ffff.ff00.0000 3Com-phone default
```

Step 3: Check the result.

#The 802.1 priority of the packets that are sent to IP Phone is modified to 7.

#PC shall not access IP Network.

### 31.3.4 Configure the lldp-med authentication mode of Voice-VLAN

#### Network Requirements

- IP Phone (it can send the LLDP packets that carry voice field) and PC access IP Network through port gigabitethernet0/1 of the Device. The MAC address of IP Phone is 0001.0001.0001, and the MAC address of PC is 0002.0002.0002.
- Configure the lldp-med authentication mode of Voice-VLAN on the Device so that IP Phone rather than PC can normally access IP Network.

#### Network Topology

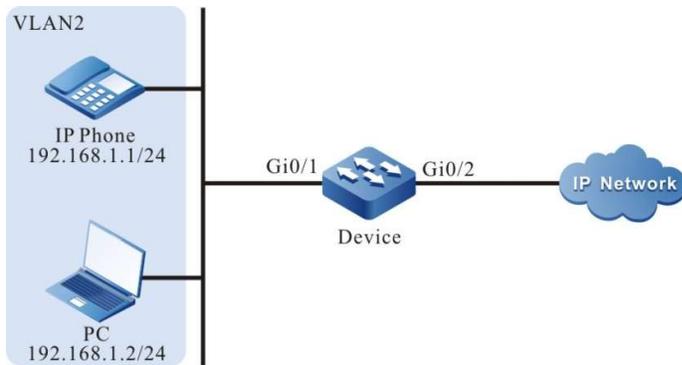


Figure 3 Configuration of Network Topology for Ildp-med Authentication Mode of Voice-VLAN

### Configuration Steps

Step 1: Configure the link type of VLAN and port.

# Create VLAN2 on Device.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the link type of port gigabitethernet0/1 on the Device as Trunk, allowing the services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode trunk
Device(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2
Device(config-if-gigabitethernet0/1)#exit
```

#Configure the link type of port gigabitethernet0/2 on the Device as Trunk, allowing the services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode trunk
Device(config-if-gigabitethernet0/2)#switchport trunk allowed vlan add 2
Device(config-if-gigabitethernet0/2)#exit
```

Step 2: Configure Voice-VLAN function.

#Configure VLAN2 as Voice-VLAN on the Device, and change corresponding value of Cos to 7.

```
Device(config)#voice vlan 2 cos 7
```

#Globally enable the Ildp-med authentication mode of Voice-VLAN on the Device.

```
Device(config)#voice vlan lldp-med authentication
```

#Configure the automatic mode of Voice-VLAN on the port gigabitethernet0/1 of the Device.

```
Device(config)# interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#voice vlan enable
Device(config-if-gigabitethernet0/1)#voice vlan mode auto
Device(config-if-gigabitethernet0/1)#exit
```

#Configure the OUI address which corresponds to the MAC address 0001.0001.0001 of IP Phone on the Device.

```
Device(config)#voice vlan oui-mac 0001.0001.0001 mask ffff.ffff.0000 name voice-vlan
```

#View the information of Voice-VLAN on the Device.

```
Device#show voice vlan all
Voice Vlan Global Information: Voice Vlan enable
Voice Vlan security: disable
Voice Vlan lldp-med authentication: enable
Voice Vlan VID: 2, Cos: 7
Default OUI number: 5
User config OUI number: 1

Voice vlan interface information:
Interface      Mode
-----
gi0/1          Auto-Mode

Voice Vlan OUI information: Total: 6
MacAddr      Mask      Name
-----
0001.0001.0000 ffff.ffff.0000 voice-vlan
0003.6b00.0000 ffff.ff00.0000 Cisco-phone default
006b.e200.0000 ffff.ff00.0000 H3C-Aolynk-phone default
00d0.1e00.0000 ffff.ff00.0000 Pingtel-phone default
00e0.7500.0000 ffff.ff00.0000 Polycom-phone default
00e0.bb00.0000 ffff.ff00.0000 3Com-phone default

Voice Vlan lldp-med authenticated mac information:
MacAddr      Interface
-----
```

```
0001.0001.0001 gi0/1
```

Step 3: Check the result.

#The 802.1 priority of the packets that are sent to IP Phone is modified to 7.

#PC shall not access IP Network.

# 32 MAC Address Table Management

---

## 32.1 Overview

A MAC address entry consists of the MAC address of a terminal, the device port that is connected to the terminal, and the ID of the VLAN to which the port belongs. After a device receives a data packet, it matches the destination MAC address of the packet with the MAC address table entries that are saved in the device so as to locate a packet forwarding port efficiently.

MAC addresses are categorized into two types: dynamic MAC addresses and static MAC addresses. Static MAC addresses are categorized into static forwarding MAC addresses and static filtering MAC addresses.

Dynamic MAC address learning is the basic MAC address learning mode of the devices. Each dynamic MAC address entry has aging time. If no packet whose source MAC address matches a MAC address entry is received by the corresponding VLAN and port, the device deletes the MAC address entry.

The dynamic MAC address learning/forwarding process is as follows:

- When a device receives a packet, it searches the MAC address table of the corresponding VLAN for the MAC address entry that matches the source MAC address of the packet. If no corresponding matching entry is available, the source MAC address of the packet is written into the MAC address table, and the aging time timer of the new MAC address entry is started. If a matching MAC address entry is found, the aging time of the MAC address entry is updated.
- In the corresponding VLAN, the device searches the MAC address table for MAC address entry that matches the destination MAC address of the packet. If no matching entry is available, the packet is flooded to the other ports with the same VLAN ID. If a matching MAC address entry is available, the packet is forwarded through the specified port.

Static filtering MAC addresses are used to isolate devices which are aggressive, preventing the devices from communicating with external devices.

The configuration/forwarding process of static filtering MAC addresses is as follows:

- Static filtering MAC addresses can only be configured by users.
- If the source MAC address or destination MAC address of a packet matches a static

filtering MAC address entry in the corresponding VLAN, the packet is discarded.

Static forwarding MAC addresses are used to control the routing principle of packets, and prevent frequent MAC address migration of MAC address entries in the table. MAC address migration means that: A device learns a MAC address from port A, then the device receives packets whose source MAC address is the same as the MAC address from port B, and port B and port A belong to the same VLAN. At this time, the forwarding port saved in the MAC address entry is updated from port A to port B.

The configuration/forwarding process of static forwarding MAC addresses is as follows:

- Static forwarding MAC addresses are configured by users.
- If the destination MAC address of a packet matches a static MAC address entry in the corresponding VLAN, the packet is forwarded through the specified port.

One port can learn the same MAC address from different VLANs, but one MAC address can only be learned by one port in one VLAN.

## 32.2 MAC Address Management Function Configuration

Table 1 MAC Address Management Function Configuration List

Configuration Task	
Configure management properties of MAC addresses.	Configure the MAC address aging time.
	Configure the MAC address learning capability.
Configure limitations on MAC address learning.	Configure limitations on port-based dynamic MAC address learning.
	Configure limitations on VLAN-based dynamic MAC address learning.
	Configure limitations on system-based dynamic MAC address learning.
Configure static MAC addresses.	Configure static filtering MAC addresses.
	Configure static forwarding MAC addresses that are bound to a port.
	Configure static forwarding MAC addresses that are bound to an aggregation group.

### 32.2.1 Configure management properties of MAC addresses.

MAC address management properties include: MAC address aging time, and the MAC address learning capability of ports.

Each dynamic MAC address entry has aging time. If no packet whose source MAC address matches a MAC address entry is received by the specified VLAN, the device deletes the MAC address entry. If the specified VLAN receives a packet whose source MAC address matches a MAC address entry, the device resets the aging time of the MAC address entry.

Static MAC addresses can only be configured and deleted by users, so static MAC addresses cannot age.

If devices in the network have idle ports and the ports do not allow free use, then the MAC address learning capability can be disabled on the port. Then, the packets received by the port will all be discarded. In this way, these ports cannot access the network, and hence the security of the network is improved.

#### Configuration Condition

None

#### Configure the MAC address aging time.

The dynamic MAC address aging time set in a device takes effect globally. The value range of the MAC address aging time is:

- 0: MAC addresses do not age, that is, the learned dynamic MAC addresses do not age.
- 10-1000000: Aging time of dynamic MAC addresses. Unit: second. Default: 300.

If the aging time is configured too long, the MAC address table in the device may contain a large number of MAC address entries that are no long in use. In this way, the large number of invalid entries may use up MAC address resources, and new valid MAC address entries fail to be added to the device. If the aging time is configured too short, the device may frequently delete valid MAC address entries, affecting the device forwarding performance. Therefore, you need to configure a reasonable value for the aging time according to the actual environment.

Table 2 Configuring MAC Address Aging Time

Step	Command	Description
Enter the global configuration mode.	<b>config terminal</b>	-
Configure the MAC address aging time.	<b>mac-address aging-time</b> <i>aging-time-value</i>	Mandatory By default, the MAC address aging time is set to 300 seconds.

### Configure the MAC address learning capability.

MAC address learning capability can be enabled and disabled only for dynamic MAC address learning. By default, the MAC address learning capability is enabled on a port. Then the port learns MAC address entries and forwards corresponding packets. If the MAC address learning capability is enabled on a port, the port does not learn dynamic MAC addresses, and the received packets are discarded.

Table 32 Configuring MAC Address Learning Capability

Step	Command	Description
Enter the global configuration mode.	<b>config terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected. After you enter the layer-2 Ethernet interface
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enable the MAC address learning capability on a port or aggregation group.	<b>mac-address learning</b>	Mandatory By default, the MAC address learning capability is enabled on a port.

### Configure the MAC address learning function

MAC address learning function can be enabled and disabled for dynamic MAC address learning packet forwarding. By default, the MAC address learning function is enabled on a port. At this moment, the port can learn MAC address entries and forward packets. If the MAC address learning function is disabled on a port, the port does not learn dynamic MAC addresses, but can still forward packets.

Table 3 Configuring MAC Address Learning Function

Step	Command	Description
Enter the global configuration mode.	<b>config terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected. After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Enable the MAC address learning function on a port or aggregation group	<b>mac-address learning action forward</b>	Mandatory By default, the MAC address learning function is enabled on a port.

### 32.2.2 Configure limitations on MAC address learning.

Limitations on MAC address learning are categorized into three types: limitations on port-based dynamic MAC address learning, limitations on VLAN-based dynamic MAC address learning, and limitations on system-based MAC address learning.

If a large number of dynamic MAC address entries have been learned by the device, it takes a long time for the device to search the MAC address table before forwarding packets, and this may cause degradation of the device performance. Therefore, you can configure limitations on dynamic MAC address learning to improve the device performance. If you configure limitations on dynamic MAC address learning on a port or VLAN, the number of access terminals can be controlled.

#### Configuration Condition

None

#### Configure limitations on port-based dynamic MAC address learning.

If the number of MAC address entries that have been learned by a port has reached the threshold value, the port discards the packets whose source MAC addresses are not in the MAC address forwarding table.

Table 32 Configuring Limitations on Port-based Dynamic MAC Address Learning

Step	Command	Description
Enter the global configuration mode.	<b>config terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected. After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Configure limitations on port-based dynamic MAC address learning.	<b>mac-address max-mac-count</b> <i>max-mac-count-value</i>	Mandatory By default, there are no limitations on dynamic MAC address learning on a port. The value range of the threshold of dynamic MAC address learning is 1-32767.

---

 **Note**

- In configuring limitations on port-based dynamic MAC address learning, if the configured threshold value is smaller than the number of existing dynamic MAC address entries on the port, the device prompts to manually clear some existing dynamic MAC address entries. After the MAC addresses are cleared, the configuration takes effect immediately.
- 

**Configure limitations on VLAN-based dynamic MAC address learning.**

If the number of MAC address entries that have been learned by a specified VLAN has reached the threshold value, the VLAN discards the packets whose source MAC addresses are not in the MAC address forwarding table.

Table 4 Configuring Limitations on VLAN-based Dynamic MAC Address Learning

Step	Command	Description
Enter the global configuration mode.	<b>config terminal</b>	-
Configure limitations on VLAN-based dynamic MAC address learning.	<b>mac-address vlan</b> <i>vlan-id</i> <b>max-mac-count</b> <i>max-mac-count-value</i>	Mandatory  By default, there are no limitations to the dynamic MAC address learning in VLAN.  The value range of the threshold of dynamic MAC address learning is 1-32767.

### Note

- In configuring limitations on VLAN-based dynamic MAC address learning, if the configured threshold value is smaller than the number of existing dynamic MAC address entries in the current VLAN, the device prompts to manually clear some existing dynamic MAC address entries. After the MAC addresses are cleared, the configuration takes effect immediately.

### Configure limitations on system-based dynamic MAC address learning.

If the number of MAC address entries that have been learned by the system has reached the threshold value, the system discards the packets whose source MAC addresses are not in the MAC address forwarding table.

Table 5 Configuring Limitations on System-based Dynamic MAC Address Learning

Step	Command	Description
Enter the global configuration mode.	<b>config terminal</b>	-
Configure limitations on system-based dynamic MAC address learning.	<b>mac-address system max-mac-count</b> <i>max-mac-count-value</i>	Mandatory  By default, MAC address learning is not limited.  The value range of the upper threshold of dynamic MAC address learning is 1-the maximum number of

Step	Command	Description
		address entries allowed to learn and supported by hardware chip.

### Note

- In configuring limitations on system-based dynamic MAC address learning, if the configured threshold value is smaller than the number of existing dynamic MAC address entries in the current system, the device prompts to manually clear some existing dynamic MAC address entries. After the MAC addresses are cleared, the configuration takes effect immediately.

### 32.2.3 Configure static MAC addresses.

Static MAC addresses are categorized into two types: static forwarding MAC addresses and static filtering MAC addresses.

The configured MAC addresses must be legal unicast MAC addresses instead of broadcast, multicast, or all-0 addresses.

One MAC address can only be configured as a static forwarding MAC address or a static filtering MAC address in a VLAN.

#### Configuration Condition

None

#### Configure static filtering MAC addresses.

After static filtering MAC address entries are configured, if the source or destination MAC addresses of the packets that are received by the corresponding VLAN match static filtering MAC address entries, the packets are discarded. This function prevents trustless devices from accessing the network, and prevents fraud and attacking activities of illegal users.

Table 6 Configuring Static Filtering MAC Address

Step	Command	Description
Enter the global configuration mode.	<b>config terminal</b>	-

Step	Command	Description
Configure static filtering MAC addresses.	<b>mac-address static</b> <i>mac-address-value</i> <b>vlan</b> <i>vlan-id</i> <b>drop</b>	Mandatory  By default, there is no static filtering MAC address in the device.

### Configure static forwarding MAC addresses that are bound to a port.

With static forwarding MAC address entries configured, after the corresponding VLAN receives packets, the port matches the destination MAC addresses of the packets with the static forwarding MAC address entries that are configured on the device. If they match successfully, the device forwards the packets through the specified port. This function helps to control the routing principle of packets more flexibly, and prevents frequent migration of MAC address entries in the table.

Table 7 Configuring Static Forwarding MAC Address Bound to a Port

Step	Command	Description
Enter the global configuration mode.	<b>config terminal</b>	-
Configure static forwarding MAC addresses that are bound to a port.	<b>mac-address static</b> <i>mac-address-value</i> <b>vlan</b> <i>vlan-id</i> <b>interface</b> <i>interface-name</i>	Mandatory  By default, no static forwarding MAC address is configured in the device.

### Configure static forwarding MAC addresses that are bound to an aggregation group.

With static forwarding MAC address entries configured, after the aggregation group receives packets, the port matches the destination MAC addresses of the packets with the static forwarding MAC address entries that are configured on the device. If they match successfully, the device forwards the packets through the specified aggregation group. This function helps to control the routing principle of packets more flexibly, and prevents frequent migration of MAC address entries in the table.

Table 8 Configuring Static Forwarding MAC Address Bound to an Aggregation Group

Step	Command	Description
Enter the global configuration mode.	<b>config terminal</b>	-

Step	Command	Description
Configure static forwarding MAC addresses that are bound to an aggregation group.	<b>mac-address static</b> <i>mac-address-value</i> <b>vlan</b> <i>vlan-id</i> <b>interface link-aggregation</b> <i>link-aggregation-id</i>	Mandatory  By default, no static forwarding MAC address is configured in the device.

### Note

- Before configuring the command, ensure that the specified aggregation group has been created.

### Configure static BPDU MAC address

After static BPDU MAC address entries are configured, if the destination MAC address values of the packets received match BPDU MAC address entries, the packets are discarded.

Table 9 Configuring Static BPDU MAC Address

Step	Command	Description
Enter the global configuration mode.	<b>config terminal</b>	-
Configure static filtering MAC addresses.	<b>mac-address bpdu</b> <i>mac-address-value</i>	Mandatory  By default, there is no static BPDU MAC address in the device.

### Note

- The following types of BPDU mac are allowed to configure:

(001) 010f-e200-0001	(002) 0180-c200-0000
(003) 0180-c200-0001	(004) 0180-c200-0002
(005) 0180-c200-0003	(006) 0180-c200-0004
(007) 0180-c200-0005	(008) 0180-c200-0006
(009) 0180-c200-0007	(010) 0180-c200-0008

(011) 0180-c200-0009	(012) 0180-c200-000a
(013) 0180-c200-000b	(014) 0180-c200-000c
(015) 0180-c200-000d	(016) 0180-c200-000e
(017) 0180-c200-000f	(018) 0180-c200-0010
(019) 0180-c200-0020/ffff-ffff-fff0	(020) 0180-c200-008a
(021) 0180-c200-8585	

### 32.2.4 MAC Address Management Monitoring and Maintaining

Table 10 MAC Address Management Monitoring and Maintaining

Command	Description
<b>clear mac-address dynamic</b> { <i>mac-address-value</i>   <b>all</b>   <b>interface</b> <i>interface-list</i>   <b>interface link-aggregation</b> <i>link-aggregation-id</i>   <b>vlan</b> <i>vlan-id</i> [ <i>mac-address-value</i>   <b>interface</b> <i>interface-list</i>   <b>interface link-aggregation</b> <i>link-aggregation-id</i> ]   <b>trill</b> <i>nickname</i> }	Clear the MAC address entries that are dynamically learned
<b>show mac-address interface</b> <i>interface-list</i> { <b>all</b>   <b>dynamic</b>   <b>static</b> [ <b>config</b> ] }	Show information of the MAC address entries on a port
<b>show mac-address interface link-aggregation</b> <i>link-aggregation-id</i> { <b>all</b>   <b>dynamic</b>   <b>static</b> [ <b>config</b> ] }	Show information of the MAC address entries in an aggregation group
<b>show mac-address vlan</b> <i>vlan-id</i> { <b>all</b>   <b>drop</b>   <b>dynamic</b>   <b>static</b> [ <b>config</b> ] }	Show information of the MAC address entries in VLAN
<b>show mac-address drop</b> [ <i>mac-address-value</i>   <b>config</b> ]	Show information of the static filtering MAC address entries in the system
<b>show mac-address dynamic</b> [ <i>mac-address-value</i> ]	Show information of the dynamic MAC address entries in the system
<b>show mac-address static</b> [ <i>mac-address-value</i>   <b>config</b> ]	Show information of the static forwarding MAC address entries in the system
<b>show mac-address system-mac</b>	Show the MAC address used by the system

Command	Description
<b>show mac-address</b> { <i>mac-address-value</i>   <b>all</b> }	Show information of the MAC address entries in the system or the specified ones
<b>show mac-address aging-time</b>	Show information of the dynamic MAC address entry aging time
<b>show mac-address max-mac-count</b> { <b>interface</b> <i>interface-name</i>   <b>interface link-aggregation</b> <i>link-aggregation-id</i>   <b>system</b>   <b>vlan</b> { <i>vlan-id</i>   <b>all</b> } }	Show information of the limitations on dynamic MAC address learning in the system
<b>show mac-address count</b> [ <b>interface</b> <i>interface-name</i>   <b>interface link-aggregation</b> <i>link-aggregation-id</i>   <b>vlan</b> <i>vlan-id</i> ]	Show statistical information of the MAC address entries in the system
<b>show mac-address bpdu</b>	Show the BPDU MAC address configured in the system
<b>show mac-address software-learning</b>	Show current MAC address learning mode of the system is software learning or hardware learning.
<b>show mac-address trill</b> { [ <i>mac-address-value</i>   <b>count</b>   <b>dynamic</b>   <b>nickname</b> [ <i>nickname</i> ]   <b>static</b>   <b>vlan</b> [ <i>vlan-id</i> ]] }	Show information of the trill mac address entries in the system
<b>show mac-address vxlan</b> [ <i>vxlan-id</i>   <b>count</b>   <b>dynamic</b>   <b>interface</b> <i>interface-list</i>   <b>ip</b> <i>ip-address</i>   <b>static</b> ]	Show information of the MAC address entries of the specified VXLAN.

## 32.3 Function configuration for software learning

### 32.3.1 Function configuration for software learning

After the software learning function is enabled, the MAC address entries are learned through software.

#### Configuration Condition

None

#### Enable software learning function

Table 11 Enabling Software Learning Function

Step	Command	Description
Enter the global configuration mode.	<b>config terminal</b>	-
Enable software learning function	<b>mac-address software-learning enable</b>	Mandatory By default, the software learning function is enabled.

### Disable software learning function

Table 12 Disabling Software Learning Function

Step	Command	Description
Enter the global configuration mode.	<b>config terminal</b>	-
Disable software learning function	<b>no mac-address software-learning enable</b>	After the software learning function is disabled, the MAC address entries are learned through chip.

### Note

- Box standalone mode, hardware learning by default. Using this command to switch to software learning.
- Rack standalone mode, hardware learning by default. Using this command to switch to software learning.
- Box stack mode, software learning by default. Using this command to switch to hardware learning.
- Rack standalone mode, hardware learning by default. Using this command to switch to software learning.
- MLAG function, supporting software learning instead of hardware learning.

## 32.3.2 Monitoring and maintenance of software learning function

Table 13 Software Learning Monitoring and Maintaining

Command	Description
<b>show mac-address software-learning</b>	View whether the status of software learning is enabled or disabled

## 32.4 Configure function of MAC address migration log

### 32.4.1 Configure function of MAC address migration log

The function of MAC address migration log can be manually enabled and disabled. After this function is enabled, when any MAC address entry has address migration, an address migration log is recorded.

#### Configuration Condition

None

#### Enable the function of MAC address migration log

Table 14 Enabling Function of MAC Address Migration Log

Step	Command	Description
Enter the global configuration mode.	<b>config terminal</b>	-
Enable the function of address migration log	<b>mac-address move log</b>	Default On

#### Disable the function of MAC address migration log

Table 15 Disabling Function of MAC Address Migration Log

Step	Command	Description
Enter the global configuration mode.	<b>config terminal</b>	-

Step	Command	Description
Disable the function of address migration log	<b>no mac-address move log</b>	After the address migration log function is disabled, the log information is not recorded when the MAC address entries have address migration.

### 32.4.2 Monitoring and maintenance of MAC address migration log function

Table 16 MAC Address Migration Monitoring and Maintaining

Command	Description
<b>clear mac-address move log</b> { <i>mac-address</i> }	Clear MAC address migration log
<b>show mac-address move config</b>	View the information about configuration of MAC address migration log function.
<b>show mac-address move log</b> { <i>mac-address-value</i>   <b>count</b> <i>count</i>   <b>hardlearn</b>   <b>interface</b> <i>interface-after</i> <b>interface</b> <i>interface-before</i>   <b>interface link-aggregation</b> <i>link-aggregation-id-after</i> <b>interface link-aggregation</b> <i>link-aggregation-id-before</i>   <b>softlearn</b>   <b>start-time</b> <i>time</i> <b>end-time</b> <i>time</i> }	View MAC address migration log.

# 33 Spanning Tree

---

## 33.1 Overview

IEEE 802.1D defines the standard Spanning Tree Protocol (STP) to eliminate network loops, preventing data frames from circulating or multiplying in loops, which may result in network congestion and affect normal communication in the network. Through the spanning tree algorithm, STP can determine where loops may exist in a network, block ports on redundant links, and trim the network into a tree structure in which no loops exist to prevent devices from receiving duplicated data frames. When the active path is faulty, STP recovers the connectivity of the blocked redundant links to ensure normal services. On the basis of STP, Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP) are developed. The basic principles of the three protocols are the same, while RSTP and MSTP are improved versions of STP. Our company has implemented the VIST and Rapid-VIST spanning tree protocols that are compatible with Cisco's spanning tree. In particular, while improving the convergence performance, Rapid-VIST inherits the function of VIST loop removal.

In STP, the following basic concepts are defined:

- Root bridge: Root of the finally formed tree structure of a network. The device with the highest priority acts as the root bridge.
- Root Port (RP): The port which is nearest to the root bridge. The port is not on the root bridge, and it communicates with the root bridge.
- Designated bridge: If the device sends Bridge Protocol Data Unit (BPDU) configuration information to a directly connected device or directly connected LAN, the device is regarded as the designated bridge of the directly connected device or directly connected LAN.
- Designated port: The designated bridge forwards BPDU configuration information through the designated port.
- Path cost: It indicates the link quality, and it is related to the link rate. Usually, a higher link rate means a smaller path cost, and the link is better.

The devices that run STP implement calculation of the spanning tree by exchanging BPDU packets, and finally form a stable topology structure. BPDU packets are categorized into the following two types:

- Configuration BPDUs: They are also called BPDU configuration messages which are

used to calculate and maintain the spanning tree topology.

- Topology Change Notification (TCN) BPDUs: When the network topology structure changes, they are used to inform other devices of the change.

BPDU packets contain information that is required in spanning tree calculation. The major information includes:

- Root bridge ID: It consists of the root bridge priority and the MAC address.
- Root path cost: It is the minimum path cost to the root bridge.
- Designated bridge ID: It consists of the designated bridge priority and the MAC address.
- Designated port ID: It consists of the designated port priority and port number.
- Message Age: Life cycle of BPDU configuration messages while they are broadcast in a network.
- Hello Time: Transmitting cycle of BPDU configuration messages.
- Forward Delay: Delay in port status migration.
- Max Age: Maximum life cycle of configuration messages in a device.

The election process of STP is as follows:

- Initial status.

The local device takes itself as the root bridge to generate BPDU configuration messages and sends the messages. In the BPDU packets, the root bridge ID and designated bridge ID are the local bridge ID, and root path cost is 0, and the specified port is the transmitting port.

Each port of the device generates a port configuration message which is used for spanning tree calculation. In the port configuration message, the root bridge ID and the designated bridge ID are the local bridge ID, the root path cost is 0, and the specified port is the local port.

- Update port configuration messages.

After the local device receives a BPDU configuration message from another device, it compares the message with the port configuration message of the receiving port. If the received configuration message is better, the device uses the received BPDU configuration message to replace the port configuration message. If the port configuration message is better, the device does not perform any operation.

The principle of comparison is as follows: The root bridge IDs, root path cost, designated bridge IDs, designated port IDs, and receiving port IDs should be compared in order. The smaller value is better. If the values of previous item are the same, compare the next item.

- Select the root bridge.

The device that sends the optimal configuration message in the entire network is selected as the root bridge.

- Select port roles and port status.

All ports of the root bridge are designated ports, and the ports are in the Forwarding status. The designated bridge selects the optimal port configuration message from all ports. The receiving port of the message is selected as the root port, and the root port is in the Forwarding status. The other ports calculate designated port configuration messages according to the root port configuration message.

The calculation method is as follows: The root bridge ID is the route ID of the root port configuration message, the root path cost is the sum of the root path cost of the root port configuration message and the root port path cost, the designated bridge ID is the bridge ID of the local device, and the designated port is the local port.

Based on the port configuration message and the calculated designated port configuration message, determine port rules: If the designated port configuration message is better, the local port is selected as the designated port, and the port is in the Forwarding status. Then, the port configuration message is replaced by the designated port configuration message, and the designated port sends port configuration messages periodically at the interval of Hello Time. If the port configuration message is better, the port is blocked. The port is then in the Discarding status, and the port configuration message is not modified.

After the root bridge, root port, and designated port are selected, the tree structure network topology is set up successfully. Only the root port and the designated port can forward data. The other ports are in the Discarding status. They can only receive configuration messages but cannot send configuration messages or forward data.

If the root port of a non-root bridge fails to receive configuration messages periodically, the active path is regarded as faulty. The device re-generates a BPDU configuration message and TCN BPDU with itself as the root bridge and sends the messages. The messages causes re-calculation of the spanning tree and then a new active path is obtained.

Before receiving new configuration messages, the other devices do not find the network topology change, so their root ports and designated port still forward data through the original path. The newly selected root port and designated port migrate to the Forwarding status after two Forward Delay periods to ensure that the new configuration message has been broadcast to the entire network and prevent occurrence of temporary loops that may be caused if both old and new root ports and designate ports forward data.

RSTP defined in IEEE 802.1w is developed based on STP, and it is the improved version of STP. RSTP realizes fast migration of port status and hence shortens the time required for a network to set up stable topology. RSTP is improved in the following aspects:

- It sets a backup port, that is, alternate port, for the root port. If the root port is blocked, the alternate port can fast switch over to become a new root port.
- It sets a backup port, that is, backup port, for the designated port. If the designated port is blocked, the backup port can fast switch over to become a new designated port.
- In a point-to-point link of two directly-connected devices, the designated port can enter the Forwarding status without delay only after a handshake with the downstream bridge.

- Some ports are not connected to the other bridges or shared links, instead, they are directly connected with user terminals. These ports are defined as edge ports. The status changes of edge ports do not affect the network connectivity, so the ports can enter the Forwarding status without delay.

However, both RSTP and STP form a single spanning tree, which has the following shortages:

- Only one spanning tree is available in the entire network. If the network size is large, the network convergence takes a long time.
- Packets of all VLANs are forwarded through one spanning tree, therefore no load balancing is achieved.

MSTP defined in IEEE 802.1s is an improvement of STP and RSTP, and it is backward compatible with STP and RSTP. MSTP introduces the concept of region and instance. MSTP divides a network into multiple regions. Each region contains multiple instances, one instance can set up mapping with one or more VLANs, and one instance corresponds to one spanning tree. One port may have different port role and status in different instances. In this way, packets of different VLANs are forwarded in their own paths.

In MSTP, definition of the following concepts is added:

- **MST domain:** It consists of multiple devices in the switching network and the network between the devices. The devices in an MST domain must meet the following requirements: The spanning tree function has been enabled on the devices. They have the same MST domain, MSTP level, and VLAN mapping table. They are directly connected physically.
- **Internal Spanning Tree (IST):** It is the spanning tree of instance 0 in each domain.
- **Common Spanning Tree (CST):** If each MST domain is regarded as a device, then the spanning trees that connect MST domains are CSTs.
- **Common and Internal Spanning Tree (CIST):** It consists of the ISTs of MST domains and the CSTs between the MST domains. It is a single spanning tree that connects all devices in the network.
- **Multiple Spanning Tree Instance (MSTI):** Spanning trees in MST domains. Each instance has an independent MSTI.
- **Common root:** CIST root.
- **Domain root:** Root of each IST and MSTI in MST domains. In MST domains, each instance has an independent spanning tree, so the domain roots may be different. The root bridge of instance 0 is the domain root of the domain.
- **Domain edge ports:** They are located at the edge of an MST domain and they are used to connect ports of different MST domains.
- **External path cost:** It is the minimum path cost from a port to the common root.
- **Internal path cost:** It is the minimum path cost from a port to the domain root.
- **Master port:** It is the domain edge port with the minimum path cost to the common

root in an MST domain. The role of a master port in an MSTI is the same as its role in a CIST.

The election rule of MSTP is similar to that of STP, that is, electing the bridge with the highest priority in the network as the root bridge of CIST by comparing configuration messages. Each MST domain calculates its IST, and MST domains calculate CSTs, and all of the constructs CIST in the entire network. Based on mapping between VLANs and spanning tree instances, each MST domain calculates an independent spanning tree MSTI for each instance.

The CISCO's private spanning tree protocol defines two protocols, i.e. PVST and RPVST. Both of them introduce the concept of instance. One VLAN corresponds to one instance. In different instances, ports may have different port roles and statuses. On this basis, different VLAN packets can be forwarded by their own path.

New definitions and precautions of MSTP in an MLAG environment:

- MLAG-MSTI: Instance MSTI corresponding to MLAG-VLAN;
- root priority: Priority of the root bridge specified by MLAG;
- bridge priority: Priority of the bridge specified by MLAG;
- stp-pseudo: Pseudo-information mode;

Restrictions on configuration of pseudo-information mode:

- The root priority (default value 0) of CIST and all MLAG-MSTIs in the pseudo-information must be higher than the bridge priority (default value 32768) of all bridges in the entire network (including MLAG node itself);
- In addition to ensuring that the partner node is the root bridge (optimal in the entire network), it is required to enable the root guard function on the access port of the MLAG node (all non-Peer-Link ports) (VIST mode does not support root guard yet) to prevent from causing errors in spanning tree calculations due to the receipt of BPDUs of higher priority.
- Bridge-Assurance function is required to be configured on the Peer-Link.
- For instances CIST and MLAG-MSTI, the root-priority of the two nodes should be the same, so that the two nodes appear as the same root bridge for both DHD and SD; in order to make the two nodes present as completely independent network bridges to SD for participation in the spanning tree calculation, the root-priority of the two nodes must be different.

## 33.2 Spanning Tree Function Configuration

Table 33 Spanning Tree Function Configuration List

Configuration Task	
Configure Basic Functions of a Spanning Tree	Enable the Spanning Tree Function
	Configure MST Domains
	Configure Spanning Tree Log Output Function
Configure Bridge Properties	Configure the Priority of a Bridge
	Configure Hello Time
	Configure Forward Delay
	Configure Max Age
	Configure the Maximum Number of Hops in an MST Domain
Configure Spanning Tree Port Properties	Configure the Priority of a Port
	Configure the Default Path Cost Standard for a Port
	Configure the Path Cost of a Port
	Configure BPDU Packet Length Check
	Configure the Maximum Length Value of BPDU Packets
	Configure the Maximum Transmitting Rate of BPDU Packets
	Configure Source MAC for BPDU Packets
	Configure Timeout Factor of BPDU Packets
	Configure an Edge Port
	Configure Automatic Detection of Edge Port
	Force Automatic Detection of Edge Port
Configure the Port Link Type	

Configuration Task	
Configure the Working Mode of a Spanning Tree	Configure the Working Mode of a Spanning Tree
Configure the Spanning Tree Protection Function	Configure the BPDU Guard Function
	Configure the BPDU Filter Function
	Configure the Flap Guard Function
	Configure the Loop Guard Function
	Configure the Root Guard Function
	Configure the TC Guard Function
	Configure the TC Protection Function

### 33.2.1 Configure Basic Functions of a Spanning Tree

#### Configuration Condition

None

#### Enable the Spanning Tree Function

After the spanning tree function is enabled, devices start to run the spanning tree protocol. The devices exchange BPDU packets to form a stable tree network topology, and network loops are eliminated.

Table 33 Enabling Spanning Tree Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enabling the spanning tree function globally.	<b>spanning-tree enable</b>	Mandatory By default, the spanning tree function is disabled globally.

Step	Command	Description
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enabling the spanning tree function on a port.	<b>spanning-tree enable</b>	Optional  By default, the spanning tree function is enabled on a port.

### Configure MST Domains

Dividing an entire network into multiple MST domains helps to shorten the network convergence time. VLAN packets are transmitted through the corresponding MSTIs in MST domains and transmitted through CSTs between MST domains.

Table 9-3 Configuring MST Domain

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the MST domain configuration mode.	<b>spanning-tree mst configuration</b>	-
Configure an MST domain name.	<b>region-name</b> <i>region-name</i>	Mandatory  By default, the name of an MST domain is the MAC address of the local device.

Step	Command	Description
Configure the MSTP revision level.	<b>revision-level</b> <i>revision-level</i>	Mandatory  By default, the MSTP revision level is 0.
Configure a VLAN mapping table.	<b>instance</b> <i>instance-id</i> <b>vlan</b> <i>vlan-list</i>	Mandatory  By default, all VLANs are mapped to instance 0.
Activate MST domain parameter configuration.	<b>active configuration pending</b>	Mandatory  By default, MST domain parameters do not take effect immediately after modification.

### Note

- MST domain parameters do not take effect immediately after they are modified. Instead, you need to run the active configuration pending command to activate the parameters and trigger re-calculation of the spanning tree. To cancel MST domain parameter configuration, use the abort configuration pending command.

### Configure Spanning Tree Log Output Function

After the spanning tree log output function is configured, when the port status changes or TC/TCN packets are received, the spanning tree directly outputs prompt logs on the device for users to quickly identify the changes of topology environment.

Table 1 Configuring Spanning Tree Log Output Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable the spanning tree log output function	<b>spanning-tree log portstate</b>	Mandatory  By default, the spanning tree log output function is disabled.

## 33.2.2 Configure Bridge Properties

### Configuration Condition

None

### Configure the Priority of a Bridge

The bridge priority and MAC address form the bridge ID. A smaller ID indicates a higher priority. The bridge with the highest priority is elected as the root bridge. One device may have different bridge priority in different spanning tree instances.

Table 2 Configuring Priority of a Bridge

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the Priority of a Bridge	<b>spanning-tree mst instance <i>instance-id</i> priority <i>priority-value</i></b>	Mandatory By default, the priority of the bridge in all spanning tree instances is 32768.
Configure the priority of a bridge under vist/rapid-vist mode	<b>spanning-tree vlan <i>vlan-id</i> priority <i>priority-value</i></b>	Mandatory By default, the priority of the bridge in all spanning tree instances is 32768.

---

### Note

- The step of bridge priorities is 4096, that is, the valid values include: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28673, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440.
- 

### Configure Hello Time

After the network topology becomes stable, the root bridge sends BPDU packets at the interval of Hello Time to inform other bridges of its role as the root bridge so that the other bridges can recognize its role. The designated bridge maintains the existing spanning tree topology according to the BPDU packet, and it forwards the BPDU packet to other devices. Generally, the designated bridge does not receive BPDU packets in a period of time as long as three times timeout period (3\*Hello Time), it regards the link as

faulty. In this way, the spanning tree re-calculates the network topology to obtain a new active path, ensuring the network connectivity.

Table 3 Configuring Hello Time

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure Hello Time	<b>spanning-tree mst hello-time seconds</b>	Mandatory By default, Hello Time is 2 seconds.
Configure Hello Time under vist/rapid-vist mode	<b>spanning-tree vlan <i>vlan-id</i> hello-time seconds</b>	Mandatory By default, Hello Time is 2 seconds.

### Note

- Forward Delay, Hello Time, and Max Age must meet the following requirement; otherwise, frequent network flapping may be cause.

$$2 \times (\text{Forward\_Delay} - 1.0\text{seconds}) \geq \text{Max\_Age}$$

$$\text{Max\_Age} \geq 2 \times (\text{Hello\_Time} + 1.0\text{seconds})$$

### Configure Forward Delay

In STP, when the root port or designated port migrates from the Discarding status to the Forwarding status, the topology change cannot be learned by the entire network immediately. To prevent temporary loops, the port migrates to the Learning status in the first Forward Delay, and then waits another Forward Delay to migrate to the Forwarding status.

Table 33 Configuring Forward Delay Time

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure Forward Delay	<b>spanning-tree mst forward-time seconds</b>	Mandatory

Step	Command	Description
		By default, Forward Delay is 15 seconds.
Configure Forward Delay Time under vist/rapid-vist mode	<b>spanning-tree vlan <i>vlan-id</i> forward-time <i>seconds</i></b>	Mandatory By default, Forward Delay is 15 seconds.

### Configure Max Age

Max Age refers to the life cycle of BPDU configuration messages while they are broadcast in a network. When a configuration message is transmitted crossing domains, after it passes through an MST domain, one is added to Message Age in the configuration message. If the device receives a configuration message and finds that the value of Message Age in the configuration message is larger than the value of Max Age, the device discards the configuration message, and the configuration message is no longer used in spanning tree calculation.

Table 4 Configuring Max Age Time

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure Max Age	<b>spanning-tree mst max-age <i>seconds</i></b>	Mandatory By default, Max Age is 20 seconds.
Configure Max Age Time under vist/rapid-vist mode	<b>spanning-tree vlan <i>vlan-id</i> max-age <i>seconds</i></b>	Mandatory By default, Max Age is 20 seconds.

### Configure the Maximum Number of Hops in an MST Domain

You can limit the size of an MST domain by configuring the maximum number of hops in the MST domain. A larger number of hops in an MST domain mean a larger MST domain. In one MST domain, starting from the domain root, once the configuration message is forwarded by a device, the number of hops is decreased by one. If the number of hops of a configuration message is 0, the device discards the configuration message. Therefore, the device which is beyond the maximum number of hops cannot participate in spanning tree calculation in the domain.

Table 5 Configuring Maximum Number of Hops in an MST Domain

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the Maximum Number of Hops in an MST Domain	<b>spanning-tree mst max-hops</b> <i>max-hops-value</i>	Mandatory  By default, the maximum number of hops in an MST domain is 20.

### 33.2.3 Configure Spanning Tree Port Properties

#### Configuration Condition

None

#### Configure the Priority of a Port

A port ID consists of port priority and port index. Port ID affects election of the port role. A smaller port ID indicates a higher priority. One port may have different port priority in different spanning tree instances.

Table 6 Configuring Priority of a Port

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.

Step	Command	Description
Configure the Priority of a Port	<b>spanning-tree mst instance</b> <i>instance-id</i> <b>port-priority</b> <i>priority-value</i>	Mandatory  By default, the priority of the port in all spanning tree instances is 128.
Configure the priority of a port under vist/rapid-vist mode	<b>spanning-tree vlan</b> <i>vlan-id</i> <b>port-priority</b> <i>priority-value</i>	Mandatory  By default, the priority of the port in all spanning tree instances is 128.

### Note

- The step of port priorities is 16, that is, the valid values include: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, and 240.

### Configure the Default Path Cost Standard for a Port

Compared with the path cost calculated based on the IEEE 802.1D-1998 standard, the path cost calculated based on the IEEE 802.1T-2001 is larger. With the increase of the link rate, the path cost value quickly decreases.

Table 7 Configuring Default Path Cost Standard for a Port

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the Default Path Cost Standard for a Port	<b>spanning-tree pathcost</b> <b>method { dot1D-1998   dot1T-2001 }</b>	Mandatory  By default, the IEEE 802.1T-2001 standard is used to calculate the default path cost of the port.

### Configure the Path Cost of a Port

The port path cost affects election of the port role. A smaller port path cost means a better link. One port may have different port path cost in different spanning tree instances.

Table 8 Configuring Port Patch Cost

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Configure the path cost of a port.	<b>spanning-tree mst instance</b> <i>instance-id</i> <b>cost</b> <i>cost-value</i>	Mandatory  By default, the path cost is automatically calculated according to the port rate.
Configure the path cost of a port under vist/rapid-vist mode	<b>spanning-tree vlan</b> <i>vlan-id</i> <b>cost</b> <i>cost-value</i>	Mandatory  By default, the path cost is automatically calculated according to the port rate.

### Configure BPDU Packet Length Check

Configure the BPDU packet length check so that the port can check the length of the received BPDU packet to prevent attacks from BPDU packets of illegal length.

Table 9 Configuring BPDU Packet Length Check

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Configure BPDU Packet Length Check	<b>spanning-tree bpdu length-check</b>	Mandatory  By default, the BPDU packet length check is disabled.

### Configure the Maximum Length Value of BPDU Packets

The maximum length value of a legal BPDU packet when BPDU packet length check is configured.

Table 10 Configuring Maximum BPDU Packet Length

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the Maximum Length Value of BPDU Packets	<b>spanning-tree bpdu max-length <i>max-length</i></b>	Mandatory  By default, the maximum length value is 1500 bytes.

### Configure the Maximum Transmitting Rate of BPDU Packets

The maximum transmitting rate of BPDU packets limits the number of BPDU packets that can be transmitted during the Hello Time of a device. This prevents the device from sending too many BPDU packets which may cause frequent spanning tree calculation for other devices.

Table 11 Configuring Maximum BPDU Packet Transmitting Rate

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the Maximum Transmitting Rate of BPDU Packets	<b>spanning-tree transmit hold-count <i>hold-count-number</i></b>	By default, the port can send 6 BPDU packets at most in Hello Time.

### Configure source MAC address check for BPDU packet

Configure source MAC address check for BPDU packet so that the port can check the source MAC address of the received BPDU packet to prevent attacks from BPDU packets of illegal device.

Table 12 Configuring Source MAC Check of BPDU Packet

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Configure Source MAC for BPDU Packets	<b>spanning-tree bpdur src-mac-match</b> <i>src-mac</i>	Mandatory  By default, the source MAC address check of BPDU packet is disabled on the port.

### Configure Timeout Factor of BPDU Packets

In a stable network topology, designated port will send a BPDU packet to neighbored device every HELLO TIME. Usually if the device doesn't receive the BPDU packet from upper devices three times beyond HELLO TIME, it is considered that the network topology changes, which will start a spanning tree re-election.

However in a stable network topology, if the upper device can't receive the BPDU packet in the case of busy or any other reason, it will start a spanning tree re-election. In this case, you can configure the timeout factor to avoid such calculation.

Table 13 Configuring Timeout Factor of BPDU Packets

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure time factor of BPDU packets	<b>spanning-tree timer-factor</b> <i>times-number</i>	By default, if the device doesn't receive the BPDU packet from upper devices three times beyond HELLO TIME, it is considered that the network topology changes, which will start a spanning tree re-election. In stacking environment, it is recommended to configure the timeout factor as 6.
Configure time factor of BPDU packet under vist/rapid-vist mode	<b>spanning-tree vlan</b> <i>vlan-id</i> <b>timer-factor</b> <i>times-number</i>	By default, if the device doesn't receive the BPDU packet from upper devices three times beyond HELLO TIME, it is considered that the network topology changes, which will start a spanning tree re-election. In stacking environment, it is recommended to configure the timeout factor as 6.

### Configure an Edge Port

Edge ports are the ports that are directly connected to user terminals. If an edge port is UP/DOWN, it does not cause temporary loops. Therefore, an edge port can quickly migrate from the Discarding status to the Forwarding status without delay time. In addition, if an edge port is UP/DOWN, it does not send TC BPDUs. This prevents unnecessary spanning tree re-calculation.

If an edge port receives BPDU packets, it becomes a non-edge port again. Then, the port can become the edge port again only after it is reset.

Table 14 Configuring Edge Port

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Configure an Edge Port	<b>spanning-tree portfast edgeport</b>	Mandatory  By default, a port is not an edge port.

---

### Note

- Before an edge port is specified, please make sure that the port is directly connected to the user terminal. Otherwise, after an edge port is configured, a temporary loop may be introduced.
- 

### Configure Automatic Detection of Edge Port

Automatic detection of edge port can be configured to automatically identify the port connected to the terminal as an edge port. This can avoid spanning tree recalculation and thus network oscillation when the terminal device goes online and offline.

An edge port will become a non-edge port again after BPDU packets are received.

Table 15 Configuring Automatic Detection of Edge Port

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Configure Automatic Detection of Edge Port	<b>spanning-tree portfast autoedge</b>	Mandatory  By default, automatic detection of edge port function is disabled in standalone and stack mode.

### Force Automatic Detection of Edge Port

Affected by the configuration or environment, current port may be identified as an edge port or a non-edge port by mistake. At this moment, users can execute this command to trigger edge port detection so that the port can correctly identify whether it is an edge port.

Table 16 Configuring Function of Forcing Automatic Detection of Edge Port

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	

Step	Command	Description
		the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Force Automatic Detection of Edge Port	<b>spanning-tree portfast autoedge force</b>	Mandatory

### Note

- This command can take effect only when the port has enabled automatic edge port detection.

### Configure the Port Link Type

If two devices are directly connected, you can configure the port link type to point-to-point link. The ports of the point-to-point link type can quickly migrate from the Discarding status to the Forwarding status without delay time.

Table 17 Configuring Link Type of Port

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected. After you enter the layer-2 Ethernet interface
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.

Step	Command	Description
Configure the Port Link Type	<b>spanning-tree link-type</b> { <b>point-to-point</b>   <b>shared</b> }	Mandatory By default, the port link type is set according to the port duplex mode. If the port works in the full duplex mode, the port is set to the point-to-point link type. If the port works in the half duplex mode, the port is set to the shared link type.

### Note

- The link type of the port should be configured according to the actual physical link. If the actual physical link of the port is not a point-to-point link, configuration as point-to-point link may bring in temporary loops.
- When the local port has a shared link, it does not support automatic identification of edge port. If automatic identification of edge port is conducted for a peer port, the peer port may be identified as an edge port by mistake.

### Configure Bridge Assurance function of the port

After the Bridge Assurance function is enabled on current port, the port will send BPDUs regardless of the spanning tree role (even if it is AlternatePort or BackupPort). If the port does not receive BPDU from the peer device for a consecutive period of time, the port status will switch to Blocking state and will not participate in the calculation of spanning tree. If BPDUs from the peer device are received later, current port will get back to normal for spanning tree calculation.

Table 18 Configuring Bridge Assurance Function of Port

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected. After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	

Step	Command	Description
		effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Configure Bridge Assurance function of the port	<b>spanning-tree bridge-assurance enable</b>	Mandatory  By default, the Bridge Assurance function of the port is disabled.

---

### Note

Restrictions on configuration of Bridge-Assurance:

- It is mutually exclusive with the port's BPDU-Guard, BPDU-Filter, and Port-Fast (adminEdge, autoEdge). If the port is configured with one of these functions, it cannot configure Bridge-Assurance (a print prompt will be given).
  - RP and AP in STP mode cannot send BPDUs at will, so the Bridge-Assurance configuration in STP mode is not effective, but it can be configured.
- 

### 33.2.4 Configure the Working Mode of a Spanning Tree

The working mode of a spanning tree determines the mode in which devices run and determines the encapsulation format of BPDU packets that are sent out. If a port that works in the MSTP mode is found to be connected to a device that runs RSTP, the port automatically migrates to the RSTP mode. If a port that works in the MSTP mode or MSTP mode is found to be connected to a device that runs STP, the port automatically migrates to the STP compatible mode.

#### Configuration Condition

None

#### Configure the Working Mode of a Spanning Tree

Table 19 Configuring Working Mode of a Spanning Tree

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the Working Mode of a Spanning Tree	<b>spanning-tree mode { stp   rstp   mstp   vist   rapid-vist}</b>	Mandatory By default, the working mode of spanning tree is MSTP.

### 33.2.5 Configure the Spanning Tree Protection Function

#### Configuration Condition

None

#### Configure the BPDU Guard Function

For an access layer device, the access port is usually directly connected to the user terminal or file server. At this time, the port is set to the edge port to realize fast migration of port statuses. When an edge port receives BPDU packets, it automatically changes to a non-edge port to cause re-generation of the spanning tree. Normally, an edge port does not receive BPDU packets. However, if someone sends faked BPDU packets to attack the device in a malicious manner, network flapping may be caused. The BPDU Guard function is used to prevent such attacks. If an edge port on which the BPDU Guard function is enabled receives BPDU packets, the port is closed.

Table 20 Configuring BPDU Guard Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected. After you enter the layer-2 Ethernet interface
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the

Step	Command	Description
		subsequent configuration takes effect only within the aggregation group.
Configure the BPDU Guard Function	<b>spanning-tree bpdu guard</b>	Mandatory By default, the BPDU Guard function is disabled.

### Configure the BPDU Filter Function

After the BPDU Filter function is enabled on an edge port, the port does not send or receive BPDU packets.

Table 21 Configuring BPDU Filter Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Configure the BPDU Filter Function	<b>spanning-tree bpdu filter</b>	Mandatory By default, the BPDU Filter function is disabled.

### Configure the Flap Guard Function

In a stable topology environment, the root port is usually not changed. However, if the links in the network are not stable or the network experiences attacks with external BPDU packets, frequent switchover of root ports may be caused, and finally network flapping is caused.

The Flap Guard function prevent frequent switchover of root ports. After the Flap Guard function is enabled, if the root port role change frequency of a spanning tree instance exceeds the specified threshold, the root port of the instance enters the Flap Guard status. In this case, the root port is always in the Discarding status, and it starts normal spanning tree calculation only after the recovery time times out.

Table 22 Configuring Flap Guard Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable the Flap Guard function	<b>spanning-tree flap-guard enable</b>	Mandatory By default, the Flap Guard function is disabled.
Configure the maximum times of change in root port allowed within the detection cycle	<b>spanning-tree flap-guard max-flaps</b> <i>max-flaps-number time seconds</i>	Optional By default, after the Flap Guard function is enabled, if a certain instance has 5 times of change in root port roles within 10 seconds, it will be under the Flap Guard status.
Configure the Flap Guard recovery time	<b>spanning-tree flap-guard recovery-time</b> <i>seconds</i>	Optional By default, Flap Guard can recover within 30 seconds.

### Configure the Loop Guard Function

The local device maintains the statuses of the root port and other blocked ports according to the BPDU packets that are periodically sent by the upstream device. In the case of link congestion or unidirectional link failure, the ports fail to receive BPDU packets from the upstream device, the spanning tree message on the port times out. Then, the downstream devices re-elect port roles. The downstream device ports that fail to receive BPDU packets change to designated port, while blocked ports migrate to the Forwarding status, resulting in loops in the switching network.

The Loop Guard function can restrain generation of such loops. After the Loop Guard function is enabled on a port, if the port times out owing to the failure to receive BPDU packets from the upstream device, in re-calculating the port role, the port is set to the Discarding status, and the port does not participate in

spanning tree calculation. If an instance on the port receives BPDU packets again, the port participates in spanning tree calculation again.

Table 23 Configuring Loop Guard Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Configure the Loop Guard Function	<b>spanning-tree guard</b> { <b>loop</b>   <b>root</b>   <b>none</b> }	Mandatory  By default, the Loop Guard function of the port is disabled.

---

 **Note**

- For Root Guard and Loop Guard of the port, only one function can be enabled.
- 

### Configure the Root Guard Function

The root bridge and backup root bridge of a spanning tree must be in the same domain, especially the CIST root bridge and its backup bridge. In network design, usually the CIST root bridge and its backup bridge are placed in the core domain with high bandwidth. However, owing to incorrect configuration or malicious attacks in the network, the legal root bridge in the network may receive a BPDU packet with a higher priority. In this way, the current legal bridge may lose its role as the root bridge, and improper change of the network topology is caused. The illegal change may lead the traffic that should be transmitted through a high-speed link to a low-speed link, causing network congestion.

The Root Guard function prevents occurrence of such case. If the Root Guard function is enabled on a port, the port can only act as the designated port in all instances. If the port receives a better BPDU configuration message, the port is set to the Discarding status. If it does not receive better BPDU configuration message in a period of time, the port resumes its previous status. It is recommended that you enable the Root Guard function on the specified port of the root bridge.

Table 24 Configuring Root Guard Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Configure the Root Guard Function	<b>spanning-tree guard</b> { <b>loop</b>   <b>root</b>   <b>none</b> }	Mandatory  By default, the Root Guard function of the port is disabled.

---

 **Note**

- For Root Guard and Loop Guard of the port, only one function can be enabled.
- 

### Configure the TC Guard Function

When a device detects a network topology change, a TC packet will be generated to notify other devices in the environment that the network topology has changed. When the device receives the TC packet, it will refresh the address. When the topology is unstable or a TC packet is manually created to launch an attack,

TC will frequently appear on the network, causing repeated address refresh of the device. This affects calculation of the spanning tree and leads to a high CPU occupancy.

TC Guard can effectively prevent this from happening. After the TC Guard is configured on current port, when the device receives the TC packet, it will no longer process the TC flag therein or spread TC, which can effectively prevent the TC packet from impacting the network.

Table 25 Configuring TC Guard Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Configure the TC Guard Function	<b>spanning-tree tc-guard enable</b>	Mandatory  By default, the TC Guard function of the port is disabled.

### Configure the TC Protection Function

If the network topology changes, to ensure normal forwarding of service data during the topology change process, when devices handle TC packets, they will refresh the MAC addresses. Attacks with faked TC packets may cause the devices to refresh MAC addresses frequently. This affects calculation of the spanning tree and leads to a high CPU occupancy.

The TC protection function prevents occurrence of such case. After the TC protection function is enabled, once a TC packet is received within the TC protection interval, the TC counter counts one. If the TC counter is equal to or larger than the threshold, it enters a suppressed status. Then, the devices do not refresh MAC addresses in handling later TC packets. After the TC protection interval, the suppressed status is changed to the normal status, and the TC counter is cleared and started again.

Table 26 Configuring TC Protection Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable the TC protection function	<b>spanning-tree tc-protection enable</b>	Optional By default, the TC protection function is enabled.
Configure the time interval of TC protection	<b>spanning-tree tc-protection interval</b> <i>seconds</i>	Mandatory By default, the time interval of TC protection is 4 seconds.
Configure the threshold value of TC protection	<b>spanning-tree tc-protection threshold</b> <i>threshold-value</i>	Mandatory By default, the threshold value of TC protection is 1.

### 33.2.6 Configure the function of configuring pseudo-information of spanning tree

#### Configuration Condition

When the pseudo-information of spanning tree is applied in the MLAG environment, on the MLAG virtual node, the conventional priority configuration method of spanning tree will not take effect. The priority of corresponding instance of the MLAG node is modified by configuring pseudo-information of spanning tree. At this moment, the instance priority information of the BPDU sent by MLAG GROUP is the pseudo-information of spanning tree configured. For the two MLAG node devices, it seems the spanning tree calculation for one device. Please note that during configuration, the pseudo-information configuration of the spanning tree on the MLAG master and standby devices should be consistent, and the configured parameters in the pseudo-information configuration mode only take effect in the MLAG environment.

#### Configure specified root bridge priority of the instance

Configure the root bridge priority of the specified spanning tree instance in pseudo-information.

Table 27 Configuring Specified Root Bridge Priority of Instance

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Configure to enter pseudo-information	<b>spanning-tree pseudo-information</b>	Mandatory
Configure the root bridge priority of the specified spanning tree instance	<b>mst instance</b> <i>instance-id</i> <b>root-priority</b> <i>priority-value</i>	Mandatory  By default, the root bridge priority of each spanning tree instance in the pseudo-information is 0 (i.e. highest priority).  <i>instance-id</i> : Spanning tree instance ID, value range 0~63  <i>priority-value</i> : Configure the root bridge priority of the device in the specified spanning tree instance. The smaller the value, the higher the priority will become.

### Note

- The step of root bridge priorities is 4096, that is, the valid values include: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440.
- On the MLAG paired device, the two devices must be consistent in terms of the root bridge priorities of all instances configured in the pseudo information.

### Configure specified bridge priority of the instance

Configure the specified bridge priority of the specified spanning tree instance in pseudo-information.

Table 28 Configuring Specified Bridge Priority of Instance

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Configure to enter pseudo-information	<b>spanning-tree pseudo-information</b>	Mandatory
Configure the specified bridge priority of the specified spanning tree instance in pseudo-information	<b>mst instance <i>instance-id</i> designated-priority <i>priority-value</i></b>	<p>Mandatory</p> <p>By default, the specified bridge priority of each spanning tree instance in the pseudo-information is configured as 32768.</p> <p><i>instance-id</i>: Spanning tree instance ID, value range 0~63</p> <p><i>priority-value</i>: Configure the root bridge priority of the device in the specified spanning tree instance. The smaller the value, the higher the priority will become.</p>

---

 **Note**

- The step of the specified bridge priorities is 4096, that is, the valid values include: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440.
- 

**Configure the root bridge priority of the specified VLAN list**

Configure the root bridge priority of the device in the specified VLAN list.

Table 29 Configuring Root Bridge Priority of Specified VLAN List

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure to enter pseudo-information	<b>spanning-tree pseudo-information</b>	Mandatory
Configure the root bridge priority of the device in the specified VLAN list	<b>spanning-tree vlan <i>vlan-list</i> root-priority <i>priority-value</i></b>	Mandatory  By default, the root bridge priority of each VLAN in the pseudo-information is 0 (i.e. highest priority).  <i>priority-value:</i> Configure the root bridge priority of the device in the specified spanning tree instance. The smaller the value, the higher the priority will become.

### Note

- The step of root bridge priorities is 4096, that is, the valid values include: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440.
- On the MLAG paired device, the two devices must be consistent in terms of the root bridge priorities of all VLANs configured in the pseudo information.

### Configure the bridge priority of the specified VLAN list

Configure the bridge priority of the device in the specified VLAN list.

Table 30 Configuring Bridge Priority of Specified VLAN List

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Configure to enter pseudo-information	<b>spanning-tree pseudo-information</b>	Mandatory
Configure bridge priority of the device in the specified VLAN list	<b>vis vlan <i>vlan-list</i> designated-priority <i>priority-value</i></b>	<p>Mandatory</p> <p>By default, the specified bridge priority of each spanning tree instance in the pseudo-information is configured as 32768.</p> <p><i>priority-value:</i> Configure the root bridge priority of the device in the specified spanning tree instance. The smaller the value, the higher the priority will become.</p>

---

 **Note**

- The step of the specified bridge priorities is 4096, that is, the valid values include: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440.
- 

### 33.2.7 Spanning Tree Monitoring and Maintaining

Table 31 Spanning Tree Monitoring and Maintaining

Command	Description
<b>clear spanning-tree detected-protocols</b>	Perform mCheck operation on the global or specified port

Command	Description
<b>clear spanning-tree bpd</b> <b>u statistics</b> [ <b>interface</b> <i>interface-name</i>   <b>interface link-aggregation</b> <i>link-aggregation-id</i> ]	Clear BPDU-related statistical information on the global or specified port
<b>show spanning-tree</b> [ <b>detail</b> ]	Show basic information of the spanning tree
<b>show spanning-tree guard</b> [ <b>current</b> [ <b>interface</b> <i>interface-name</i>   <b>interface link-aggregation</b> <i>link-aggregation-id</i> ]]	Show configuration and status information of the spanning tree protection function on the port
<b>show spanning-tree</b> { <b>interface</b> <i>interface-name</i>   <b>interface link-aggregation</b> <i>link-aggregation-id</i> } [ <b>detail</b> ]	Show spanning tree status information of the specified port or aggregation group
<b>show spanning-tree mst</b> [ <b>configuration</b> [ <b>current</b>   <b>pending</b> ]   <b>detail</b>   <b>instance</b> <i>instance-id</i> [ <b>detail</b> ]   { <b>interface</b> <i>interface-name</i>   <b>interface link-aggregation</b> <i>link-aggregation-id</i> } [ <b>instance</b> <i>instance-id</i> ] ]	Show spanning tree configuration and status information
<b>show configuration</b> { <b>current</b>   <b>pending</b> }	Show related configuration of MST Domain
<b>show spanning-tree vlan</b> <i>vlan-id</i> [ <b>detail</b> ]	Show spanning tree status information of the specified vlan in vist/rapid-vist mode

## 33.3 Spanning Tree Typical Configuration Example

### 33.3.1 MSTP Typical Application

#### Network Requirements

- Four devices in the network are in the same MST domain. Device1 and Device2 are convergence layer devices, while Device3 and Device4 are access layer devices.
- To reasonably balance traffic on the links to realize load sharing and redundancy backup, configure packets of VLAN2 to be forwarded following instance 1. The root bridge of instance 1 is Device1. Packets of VLAN3 are forwarded following instance 2. The root bridge of instance 2 is Device2. Packets of VLAN4 are forwarded following instance 0.

## Network Topology

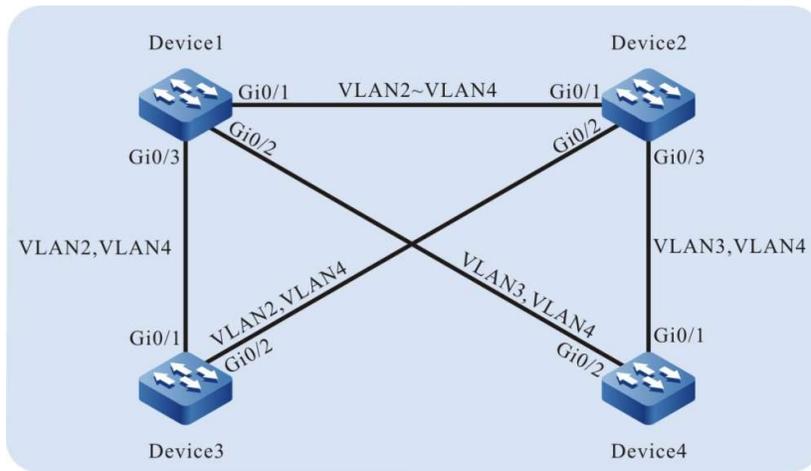


Figure 1 Network Topology for Typical Application of MSTP

### Configuration Steps

*Step 1:* Configure VLANs, and configure the link type of the ports.

#On Device1, create VLAN2-VLAN4, configure the link type of port gigabitethernet0/1 to Trunk and allow services of VLAN2-VLAN4 to pass.

```
Device1(config)#vlan 2-4
Device1(config)#interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#switchport mode trunk
Device1(config-if-gigabitethernet0/1)#switchport trunk allowed vlan add 2-4
Device1(config-if-gigabitethernet0/1)#exit
```

#On Device1, configure the link type of port gigabitethernet0/2 as Trunk and allow services of VLAN3 and VLAN4 to pass. Configure the link type of port gigabitethernet0/3 as Trunk and allow services of VLAN2 and VLAN4 to pass. (Omitted)

#On Device2, create VLAN2-VLAN4. Configure the link type of ports gigabitethernet0/1-gigabitethernet0/3 to Trunk, configure gigabitethernet0/1 to allow services of VLAN2-VLAN4 to pass, gigabitethernet0/2 to allow services of VLAN2 and VLAN4 to pass, and gigabitethernet0/3 to allow services of VLAN3 and VLAN4 to pass. (Omitted)

#On Device3, create VLAN2 and VLAN4. Configure the link type of ports gigabitethernet0/1~gigabitethernet0/2 as Trunk, allowing the services of VLAN2 and VLAN4 to pass. (Omitted)

#On Device4, create VLAN3 and VLAN4. Configure the link type of ports gigabitethernet0/1~gigabitethernet0/2 as Trunk and allow services of VLAN3 and VLAN4 to pass. (Omitted)

*Step 2:* Configure an MST domain.

#On Device1, configure an MST domain. Set the domain name to admin, the revision level to 1, map instance 1 to VLAN2, map instance 2 to VLAN3, and activate the MST domain.

```
Device1#configure terminal
Device1(config)#spanning-tree mst configuration
Device1(config-mst)#region-name admin
Device1(config-mst)#revision-level 1
Device1(config-mst)#instance 1 vlan 2
Device1(config-mst)#instance 2 vlan 3
Device1(config-mst)#active configuration pending
Device1(config-mst)#exit
```

---

### Note

- The MST domain configuration of Device2, Device3, and Device 4 is the same as that of Device1. (Omitted)
- 

#On Device1, configure the priority of MSTI 1 to 0. On Device2, configure the priority of MSTI 2 to 0.

```
Device1(config)#spanning-tree mst instance 1 priority 0
Device2(config)#spanning-tree mst instance 2 priority 0
```

#On Device1, enable the spanning tree globally.

```
Device1(config)#spanning-tree enable
```

---

### Note

- The configuration for enabling the spanning tree globally on Device2, Device3, and Device 4 is the same as that on Device1. (Omitted)
- 

*Step*  
3:

Check the result.

#After the network topology is stable, check the calculation result of all spanning tree instances.

```
Device1#show spanning-tree mst
Spanning-tree enabled protocol mstp
MST Instance 00    vlans mapped: 1,4-4094
Bridge            address 0000.0000.008b priority 32768
Region root      address 0000.0000.008b priority 32768
  Designated root address 0000.0000.008b priority 32768
                  root: 0, rpc: 0, epc: 0, hop: 20
Operational hello time 2, forward time 15, max age 20
Configured hello time 2, forward time 15, max age 20, max hops 20, hold count 6
Flap guard : admin false, max count 5, detect period 10s, recovery period 30s
Tc protection: admin true, threshold 3, interval 2s, rxTcCnt 0, status:NORMAL
Bpdu length-check: false, bpdu illegal length packets count: 0
Autoedge swap-check: true
Swap-delay time: 30
Configured timer factor: 3
```

```

Topology Change Count:4, last change occurred:0 hour 1 minute 0 second(60 seconds)
-----
Interface Role Sts Cost Prio.Nbr Type
-----
gi0/1      Desg FWD  20000 128.001 P2P
gi0/2      Desg FWD  20000 128.002 P2P
gi0/3      Desg FWD  20000 128.003 P2P
MST Instance 01 vlans mapped: 2
Bridge ID   address 0000.0000.008b priority 1/0
Designated root address 0000.0000.008b priority 1
              root: 0, rpc: 0, hop: 20
Topology Change Count:4, last change occurred:0 hour 1 minute 0 second(60 seconds)
-----
Interface Role Sts Cost Prio.Nbr Type
-----
gi0/1      Desg FWD  20000 128.001 P2P
gi0/3      Desg FWD  20000 128.003 P2P
MST Instance 02 vlans mapped: 3
Bridge ID   address 0000.0000.008b priority 32770/32768
Designated root address 0001.7a54.5c96 priority 2
              root: 32769, rpc: 20000, hop: 19
Topology Change Count:4, last change occurred:0 hour 1 minute 0 second(60 seconds)
-----
Interface Role Sts Cost Prio.Nbr Type
-----
gi0/1      Root FWD  20000 128.001 P2P
gi0/2      Desg FWD  20000 128.002 P2P

```

#On Device2, query the calculation result of all spanning tree instances. According to the result, port gigabitethernet0/2 of Device2 is blocked in both instance 0 and instance 1.

```

Device2#show spanning-tree mst
Spanning-tree enabled protocol mstp
MST Instance 00 vlans mapped: 1,4-4094
Bridge address 0001.7a54.5c96 priority 32768
Region root address 0000.0000.008b priority 32768
Designated root address 0000.0000.008b priority 32768
              root: 32769, rpc: 20000, epc: 0, hop: 19
Operational hello time 2, forward time 15, max age 20
Configured hello time 2, forward time 15, max age 20, max hops 20, hold count 6
Flap guard : admin false, max count 5, detect period 10s, recovery period 30s
Tc protection: admin true, threshold 3, interval 2s, rxTcCnt 0, status:NORMAL
Bpdu length-check: false, bpdu illegal length packets count: 0
Autoedge swap-check: true
Swap-delay time: 30
Configured timer factor: 3
Topology Change Count:4, last change occurred:0 hour 1 minute 0 second(60 seconds)
-----
Interface Role Sts Cost Prio.Nbr Type
-----
gi0/1      Root FWD  20000 128.001 P2P
gi0/2      Alte DIS  20000 128.002 P2P
gi0/3      Desg FWD  20000 128.003 P2P
MST Instance 01 vlans mapped: 2
Bridge ID   address 0001.7a54.5c96 priority 32769/32768
Designated root address 0000.0000.008b priority 1
              root: 32769, rpc: 20000, hop: 19
Topology Change Count:4, last change occurred:0 hour 1 minute 0 second(60 seconds)
-----
Interface Role Sts Cost Prio.Nbr Type
-----
gi0/1      Root FWD  20000 128.001 P2P
gi0/2      Alte DIS  20000 128.002 P2P
MST Instance 02 vlans mapped: 3
Bridge ID   address 0001.7a54.5c96 priority 2/0
Designated root address 0001.7a54.5c96 priority 2
              root: 0, rpc: 0, hop: 20
Topology Change Count:4, last change occurred:0 hour 1 minute 0 second(60 seconds)
-----
Interface Role Sts Cost Prio.Nbr Type
-----
gi0/1      Desg FWD  20000 128.001 P2P
gi0/3      Desg FWD  20000 128.003 P2P

```

#On Device3, query the calculation result of all spanning tree instances.

```

Device3#show spanning-tree mst
Spanning-tree enabled protocol mstp
MST Instance 00    vlans mapped: 1,4-4094
Bridge            address 0000.0305.070a priority 32768
Region root      address 0000.0000.008b priority 32768
  Designated root address 0000.0000.008b priority 32768
                  root: 32769, rpc: 20000, epc: 0, hop: 19
Operational hello time 2, forward time 15, max age 20
Configured hello time 2, forward time 15, max age 20, max hops 20, hold count 6
Flap guard : admin false, max count 5, detect period 10s, recovery period 30s
Tc protection: admin true, threshold 3, interval 2s, rxTcCnt 0, status:NORMAL
Bpdu length-check: false, bpdu illegal length packets count: 0
Autoedge swap-check: true
Swap-delay time: 30
Configured timer factor: 3
Topology Change Count:4, last change occurred:0 hour 1 minute 0 second(60 seconds)
-----
Interface Role Sts Cost Prio.Nbr Type
-----
gi0/1      Root FWD  20000 128.001 P2P
gi0/2      Desg FWD  20000 128.002 P2P
MST Instance 01    vlans mapped: 2
Bridge ID      address 0000.0305.070a priority 32769/32768
Designated root address 0000.0000.008b priority 1
                root: 32769, rpc: 20000, hop: 19
Topology Change Count:4, last change occurred:0 hour 1 minute 0 second(60 seconds)
-----
Interface Role Sts Cost Prio.Nbr Type
-----
gi0/1      Root FWD  20000 128.001 P2P
gi0/2      Desg FWD  20000 128.002 P2P

```

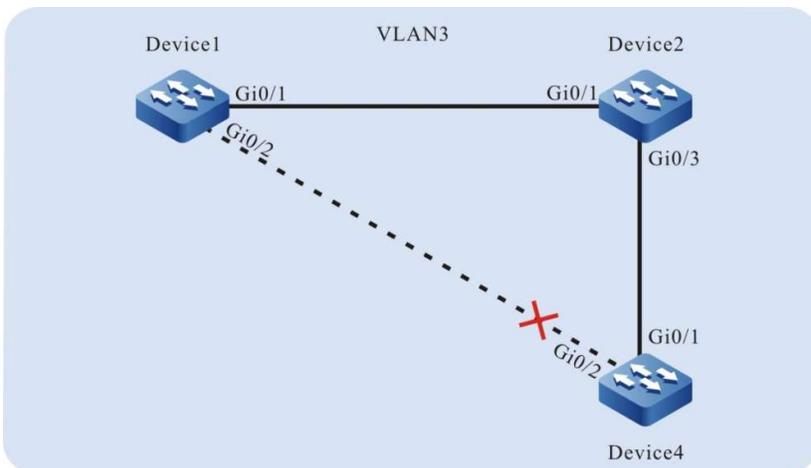
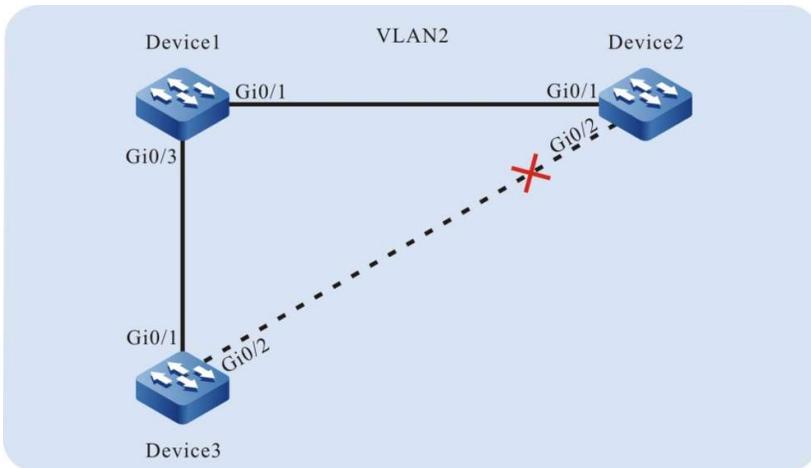
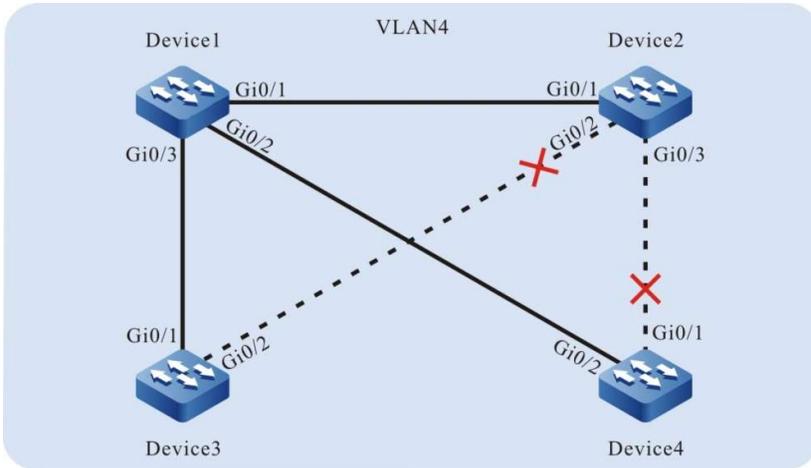
#On Device4, query the calculation result of all spanning tree instances. According to the result, port gigabitethernet0/1 of Device4 is blocked in instance 0, and port gigabitethernet0/2 is blocked in instance 2.

```

Device4#show spanning-tree mst
Spanning-tree enabled protocol mstp
MST Instance 00    vlans mapped: 1,4-4094
Bridge            address 0001.7a58.dc0c priority 32768
Region root      address 0000.0000.008b priority 32768
  Designated root address 0000.0000.008b priority 32768
                  root: 32769, rpc: 20000, epc: 0, hop: 19
Operational hello time 2, forward time 15, max age 20
Configured hello time 2, forward time 15, max age 20, max hops 20, hold count 6
Flap guard : admin false, max count 5, detect period 10s, recovery period 30s
Tc protection: admin true, threshold 3, interval 2s, rxTcCnt 0, status:NORMAL
Bpdu length-check: false, bpdu illegal length packets count: 0
Autoedge swap-check: true
Swap-delay time: 30
Configured timer factor: 3
Topology Change Count:4, last change occurred:0 hour 1 minute 0 second(60 seconds)
-----
Interface Role Sts Cost Prio.Nbr Type
-----
gi0/1      Alte DIS  20000 128.001 P2P
gi0/2      Root FWD  20000 128.002 P2P
MST Instance 02    vlans mapped: 3
Bridge ID      address 0001.7a58.dc0c priority 32770/32768
Designated root address 0001.7a54.5c96 priority 2
                root: 32769, rpc: 20000, hop: 19
Topology Change Count:4, last change occurred:0 hour 1 minute 0 second(60 seconds)
-----
Interface Role Sts Cost Prio.Nbr Type
-----
gi0/1      Root FWD  20000 128.001 P2P
gi0/2      Alte DIS  20000 128.002 P2P

```

Based on the spanning tree calculation result of the four devices, the tree diagrams corresponding to MSTI 0 (mapped to VLAN4), MSTI 1 (mapped to VLAN2), and MSTI 2 (mapped to VLAN3) are obtained.



### 33.3.2 Application of basic MSTP functions in the MLAG environment

#### Network Requirements

- The 4 devices on the network are within the same MST domain, with the network

bridge priority of MLAG device being the highest.

## Network Topology

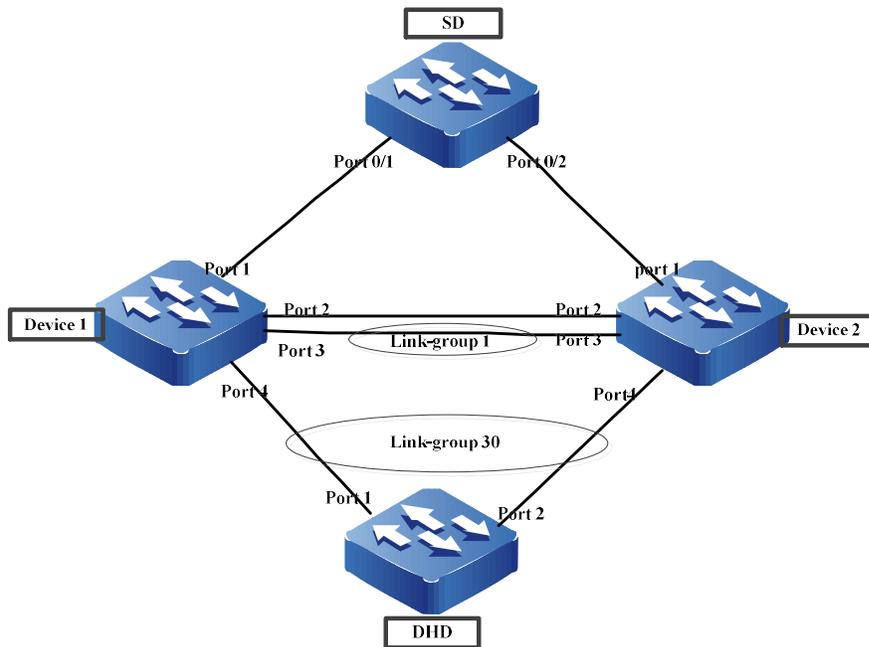


Figure 2 Network Topology for Application of MSTP in MLAG

## Configuration Steps

Step 1: Add the interface into the aggregation group and vlan. (Omitted)

Step 2: Configure MLAG domain. (Omitted)

Step 3: Configure MST domain

#On Device1, configure an MST domain. Set the domain name to admin and revision level to 1, and activate the MST domain.

```
Device1#configure terminal
Device1(config)#spanning-tree mst configuration
Device1(config-mst)#region-name admin
Device1(config-mst)#revision-level 1
Device1(config-mst)#active configuration pending
Device1(config-mst)#exit
```

---

### Note

- The MST domain configuration of Device2, SD, and DHD is the same as that of Device1. (Omitted)
-

View information about the spanning tree of each device

#Convergence 1 on #DEVICE1 and DEVICE2 is an inline port

```
Device1#show spanning-tree
Spanning-tree enabled protocol mstp
MST Instance 00      vlans mapped: 1-4094
Bridge              address 0001.7a95.000b priority 0
Region root         address 0001.7a95.000b priority 0
Designated root     address 0001.7a95.000b priority 0
                    root: 0, rpc: 0, epc: 0, hop: 20
                    We are the root of the spanning tree
Operational hello time 2, forward time 15, max age 20, message age 0
Configured  hello time 2, forward time 15, max age 20, max hops 20, hold count 10
Flap guard : admin false, max count 5, detect period 10s, recovery period 30s
Tc protection: admin true, threshold 2, interval 20s, rxTcCnt 0, status:NORMAL
ARL flush: enabled
Bpdu length-check: false, bpdu illegal length packets count: 0
Autoedge swap-check: true
Swap-delay time: 30
Configured timer factor: 3
Topology Change Count:6, last change occurred:118 weeks 5 days(71863322 seconds)
Interface      Role Sts Cost   Prio.Nbr Type
-----
te0/1          Desg FWD 20000 128.0036 P2P
link-agg1      Desg FWD 1950   128.0193 P2P (MLAG peer-link)
link-agg30     Desg FWD 19500 128.0222 P2P (MLAG 100)
```

```
Device2#show spanning-tree
Spanning-tree enabled protocol mstp
MST Instance 00      vlans mapped: 1-4094
Bridge              address 0001.7a95.000b priority 0
Region root         address 0001.7a95.000b priority 0
Designated root     address 0001.7a95.000b priority 0
                    root: 0, rpc: 0, epc: 0, hop: 20
                    We are the root of the spanning tree
Operational hello time 2, forward time 15, max age 20, message age 0
Configured  hello time 2, forward time 15, max age 20, max hops 20, hold count 6
Flap guard : admin false, max count 5, detect period 10s, recovery period 30s
Tc protection: admin true, threshold 1, interval 4s, rxTcCnt 0, status:NORMAL
ARL flush: enabled
Bpdu length-check: false, bpdu illegal length packets count: 0
Autoedge swap-check: true
Swap-delay time: 30
Configured timer factor: 3
Topology Change Count:7, last change occurred:118 weeks 4 days(71776558 seconds)
Interface      Role Sts Cost   Prio.Nbr Type
-----
gi0/1          Desg FWD 20000 128.0332 P2P
link-agg1      IRoot FWD 1950   128.0385 P2P (MLAG peer-link)
link-agg30     Desg FWD 19500 128.0414 P2P (MLAG 100)
```

#The port spanning tree where SD connects to Device2 is calculated as block, and the mlag-group connected to DHD as Root

```
SD#show spanning-tree
Spanning-tree enabled protocol mstp
MST Instance 00      vlans mapped: 1-4094
Bridge              address 0001.7a7a.3c10 priority 32768
Region root         address 0001.7a95.000b priority 0
Designated root     address 0001.7a95.000b priority 0
                    root: 32804, rpc: 20000, epc: 0, hop: 19
Operational hello time 2, forward time 15, max age 20, message age 0
Configured  hello time 2, forward time 15, max age 20, max hops 20, hold count 6
Flap guard : admin false, max count 5, detect period 10s, recovery period 30s
Tc protection: admin true, threshold 1, interval 4s, rxTcCnt 0, status:NORMAL
ARL flush: enabled
Bpdu length-check: false, bpdu illegal length packets count: 0
```

```

Autoedge swap-check: true
Swap-delay time: 30
Configured timer factor: 1
Topology Change Count:36, last change occurred:118 weeks 5 days(71863036 seconds)
Interface      Role Sts Cost   Prio.Nbr Type
-----
gi0/1         Root FWD 20000   128.0012 P2P
gi0/2         Alte DIS 20000   128.0036 P2P

DHD#show spanning-tree
Spanning-tree enabled protocol mstp
MST Instance 00    vlans mapped: 1-4094
Bridge           address 0001.7a6a.0148 priority 32768
Region root      address 0001.7a95.000b priority 0
Designated root  address 0001.7a95.000b priority 0
                  root: 33662, rpc: 18000, epc: 0, hop: 19
Operational hello time 2, forward time 15, max age 20, message age 0
Configured hello time 2, forward time 15, max age 20, max hops 20, hold count 6
Flap guard : admin false, max count 5, detect period 10s, recovery period 30s
Tc protection: admin true, threshold 1, interval 4s, rxTcCnt 0, status:NORMAL
ARL flush: enabled
Bpdu length-check: false, bpdu illegal length packets count: 0
Autoedge swap-check: true
Swap-delay time: 30
Configured timer factor: 6
Topology Change Count:20, last change occurred:118 weeks 5 days(71863409 seconds)
Interface      Role Sts Cost   Prio.Nbr Type
-----
link-agg30     Root FWD 18000   128.0894 P2P

```

Step 4: Modify the specified bridge priority of Device2 so that the blocked port of SD is calculated as 0/1.

```

Device2#conf t
Device2(config)#spanning-tree pseudo-information
Device2 (config-stp-pseudo)#mst instance 0 designated-priority 4096

SD# show spanning-tree
Spanning-tree enabled protocol mstp
MST Instance 00    vlans mapped: 1-4094
Bridge           address 0001.7a7a.3c10 priority 32768
Region root      address 0001.7a95.000b priority 0
Designated root  address 0001.7a95.000b priority 0
                  root: 32780, rpc: 20000, epc: 0, hop: 19
Operational hello time 2, forward time 15, max age 20, message age 0
Configured hello time 2, forward time 15, max age 20, max hops 20, hold count 6
Flap guard : admin false, max count 5, detect period 10s, recovery period 30s
Tc protection: admin true, threshold 1, interval 4s, rxTcCnt 0, status:NORMAL
ARL flush: enabled
Bpdu length-check: false, bpdu illegal length packets count: 0
Autoedge swap-check: true
Swap-delay time: 30
Configured timer factor: 1
Topology Change Count:37, last change occurred:118 weeks 5 days(71864200 seconds)
Interface      Role Sts Cost   Prio.Nbr Type
-----
gi0/1         Root FWD 20000   128.0012 P2P
gi0/2         Alte DIS 20000   128.0036 P2P

```

Step 5: Enable BA function on the inline port of Device1 and Device2

```

Device1(config)#interface link-aggregation 1
Device1(config-if-link-aggregation1)#spanning-tree bridge-assurance enable
Device2(config)#interface link-aggregation 1
Device2(config-if-link-aggregation1)#spanning-tree bridge-assurance enable

```

# 34 Loopback Detection

---

## 34.1 Overview

In the Ethernet, if the destination of some packet fails to be recognized, they will be flooded in a VLAN. If a loop exists in the network, the packets circulate and multiply without limit, and finally they will use up the bandwidth. Then, the network fails to provide normal communication.

There are two types of loops, loop between different ports of a device, and loop on one port of a device. The two types of loops can be detected through loopback detection.

After the loopback detection function is enabled, a port sends loopback detection packets at intervals in the VLAN to which it has been added to check whether a loop exists in the network. When a port receives a loopback detection packet that the local device sent, it determines that a loop exists in the network. Then, the port is disabled to prevent the local loop from affecting the entire network.

## 34.2 Loopback Detection Function Configuration

Table 34 Loopback Detection Function Configuration List

Configuration Task	
Configure basic functions of loopback detection.	Enable the global loopback detection control switch.
	Enable the loopback detection control switch of a port or aggregation group.
Configure basic parameters of loopback detection.	Configure the interval at which loopback detection packets are sent.
	Configure the Error-Disable action on a port.

### 34.2.1 Configure basic functions of loopback detection.

#### Configuration Condition

None

#### Enable the global loopback detection control switch.

The global loopback detection control switch is used to enable the global loopback detection function. The loopback detection configuration of a port takes effect only after the global loopback detection control switch is enabled.

Table 34 Enabling Global Loopback Detection Control Switch

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable the global loopback detection control switch.	<b>loopback-detection enable</b>	Mandatory By default, the global loopback detection control switch is disabled.

#### Enable the loopback detection control switch of a port or aggregation group.

After the loopback detection function is enabled, a port sends loopback detection packets at intervals in the VLAN to which it has been added to check whether a loop exists in the network.

Table 34 Enabling Loopback Detection Control Switch of a Port or Aggregation Group

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2/3 Ethernet interface configuration mode	<b>interface</b> <i>interface-name</i>	At least one option must be selected. After you enter the layer-2/3 Ethernet interface configuration mode, the subsequent
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	

Step	Command	Description
		configuration takes effect only on current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enable the loopback detection control switch of a port or aggregation group.	<b>loopback-detection enable</b>	Mandatory  By default, the loopback detection control switch of a port or aggregation group is disabled.

---

 **Note**

- In loopback detection configuration task, you must enable the global loopback detection control switch before the loopback detection configuration on a port takes effect.
- 

### 34.2.2 Configure basic parameters of loopback detection.

#### Configuration Condition

None

#### Configure the interval at which loopback detection packets are sent.

In a loopback detection, loopback detection packets are sent periodically to detect loops in the network. You can modify the interval at which loopback detection packets are sent according to the actual network requirement.

Table 34 Configuring Interval at Which Loopback Detection Packets Are Sent

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2/3 Ethernet interface configuration mode	<b>interface</b> <i>interface-name</i>	At least one option must be selected.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	After you enter the layer-2/3 Ethernet interface configuration mode, the subsequent configuration takes effect only on current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Configure the interval at which loopback detection packets are sent.	<b>loopback-detection enable interval-time</b> <i>interval-time-value</i>	Mandatory  By default, the interval at which loopback detection packets are sent is 30 seconds.

### Configure the Error-Disable action on a port.

If a port allows the Error-Disable action, the port is controlled. After a port detects a loop, it performs the Error-Disable action to close the port so as to eliminate the loop. If the port is not in the controlled status, the port only prints loop prompt message instead of closing the port. In this case, the loop has not been eliminated.

Table 34 Configuring Error-disable Action on a Port

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2/3 Ethernet interface configuration mode	<b>interface</b> <i>interface-name</i>	At least one option must be selected. After you enter the layer-2/3 Ethernet interface configuration mode, the subsequent configuration takes effect only on current port.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Configure whether the port allows the Error-Disable function.	<b>loopback-detection enable control</b>	Mandatory By default, after a port detects a loop, it performs the Error-Disable action.

### 34.2.3 Loopback Detection Monitoring and Maintaining

Table 34 Loopback Detection Monitoring and Maintaining

Command	Description
<b>show loopback-detection</b> [ <b>interface</b> <i>interface-name</i>   <b>interface link-aggregation</b> <i>link-aggregation-id</i> ]	Displays the configuration information of all ports or a specified port in loopback detection.

## 34.3 Typical Configuration Example of Loopback Detection

### 34.3.1 Configure Remote Loopback Detection

#### Network Requirements

- Device1 and Device2 are directly connected, and Device2 has two ports which form a self-loop.
- On Device1, loopback detection has been enabled.
- After Device1 detects a loop, it closes the interconnected port to eliminate the loop.

#### Network Topology

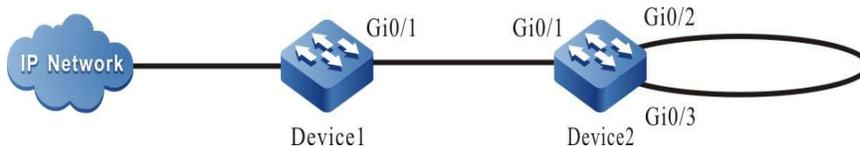


Figure 34 Network Topology for Configuration of Remote Loopback Detection Function

#### Layer-2 Ethernet interface configuration steps

Step 1: Configure the link type of VLAN and layer-2 Ethernet interface.

#Create VLAN2 on Device1.

```
Device1#configure terminal
Device1(config)#vlan 2
Device1(config-vlan2)#exit
```

#Configure the link type of layer-2 Ethernet interface gigabitethernet0/1 on Device1 as Trunk, allowing the services of VLAN2 to pass.

```
Device1(config)#interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#switchport mode trunk
Device1(config-if-gigabitethernet0/1)#switchport trunk allowed vlan add 2
Device1(config-if-gigabitethernet0/1)#exit
```

#Create VLAN2 on Device2.

```
Device2#configure terminal
Device2(config)#vlan 2
Device2(config-vlan2)#exit
```

#Configure the link type of layer-2 Ethernet interfaces gigabitethernet0/1, gigabitethernet0/2 and gigabitethernet0/3 on Device2 as Trunk, allowing the services of VLAN2 to pass and the layer-2 Ethernet interfaces gigabitethernet0/2 and gigabitethernet0/3 to disable the spanning tree.

```

Device2(config)#interface gigabitethernet 0/1-0/3
Device2(config-if-range)#switchport mode trunk
Device2(config-if-range)#no switchport trunk allowed vlan 1
Device2(config-if-range)#switchport trunk allowed vlan add 2
Device2(config-if-range)#exit
Device2(config)#interface gigabitethernet 0/2-0/3
Device2(config-if-range)#no spanning-tree enable
Device2(config-if-range)#exit

```

Step 2: Enable the loopback detection function.

#On Device1, globally enable the loopback detection function.

```
Device1(config)#loopback-detection enable
```

#On Device1, view the loopback detection status.

```

Device1#show loopback-detection
-----
Global loopback-detection : ENABLE
-----
Interface      Loopback Time(s) State      Control
-----
gi0/1          DISABLE  30    NORMAL    TRUE
gi0/2          DISABLE  30    NORMAL    TRUE

```

#Enable the loopback detection function on the layer-2 Ethernet interface gigabitethernet0/1 of Device1.

```

Device1(config)#interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#loopback-detection enable
Device1(config-if-gigabitethernet0/1)#exit

```

Step 3: Check the result.

#On Device1, view the loopback detection status.

```

After a loop is detected:
Device1#show loopback-detection
-----
Global loopback-detection : ENABLE
-----
Interface      Loopback Time(s) State      Control
-----
gi0/1          ENABLE   30    ERR-DISABLE TRUE
gi0/2          DISABLE  30    NORMAL    TRUE

```

#After Device1 detects a loop, the layer-2 Ethernet interface gigabitethernet0/1 performs close operation, and the following prompt messages are output on the device.

```

Jul 30 2014 03:30:30: %LOOP-BACK-DETECTED : loop-back send tag packet in vlan2 on gigabitethernet0/1, detected in vlan2
from gigabitethernet0/1
Jul 30 2014 03:30:30: %LINK-INTERFACE_DOWN-4: interface gigabitethernet0/1, changed state to down
Jul 30 2014 03:30:30: %LINEPROTO-5-UPDOWN : gigabitethernet0/1 link-status changed to err-disable

```

#Check the status of layer-2 Ethernet interface gigabitethernet0/1 on Device1. The link status of layer-2 Ethernet interface gigabitethernet0/1 becomes Down.

```

Device1#show interface gigabitethernet 0/1
gigabitethernet0/1 configuration information
Description :

```

```

Status      : Enabled
Link        : Down (Err-disabled)
Set Speed   : Auto
Act Speed   : Unknown
Set Duplex  : Auto
Act Duplex  : Unknown
Set Flow Control : Off
Act Flow Control : Off
Mdix        : Auto
Mtu         : 1824
Port mode   : LAN
Port ability : 10M HD,10M FD,100M HD,100M FD,1000M FD
Link Delay  : No Delay
Storm Control : Unicast Disabled
Storm Control : Broadcast Disabled
Storm Control : Multicast Disabled
Storm Action : None
Port Type   : Nni
Pvid        : 1
Set Medium  : Copper
Act Medium  : Copper
Mac Address : 0000.0000.008b

```

### Layer-3 Ethernet interface configuration steps

Step 1: Configure the link type of VLAN and layer-2 Ethernet interface.

#Create VLAN2 on Device2.

```

Device2#configure terminal
Device2(config)#vlan 2
Device2(config-vlan2)#exit

```

#Configure the link type of layer-2 Ethernet interfaces gigabitethernet0/1, gigabitethernet0/2 and gigabitethernet0/3 on Device2 as Trunk, allowing the services of VLAN2 to pass and the layer-2 Ethernet interfaces gigabitethernet0/2 and gigabitethernet0/3 to disable the spanning tree.

```

Device2(config)#interface gigabitethernet 0/1-0/3
Device2(config-if-range)#switchport mode trunk
Device2(config-if-range)#no switchport trunk allowed vlan 1
Device2(config-if-range)#switchport trunk allowed vlan add 2
Device2(config-if-range)#switchport trunk pvid vlan 2
Device2(config-if-range)#exit
Device2(config)#interface gigabitethernet 0/2-0/3
Device2(config-if-range)#no spanning-tree enable
Device2(config-if-range)#exit

```

Step 2: Enable the loopback detection function.

#On Device1, globally enable the loopback detection function.

```

Device1(config)#loopback-detection enable

```

#On Device1, view the loopback detection status.

```

Device1#show loopback-detection
-----
Global loopback-detection : ENABLE

```

```

-----
Interface      Loopback Time(s) State      Control
-----
gi0/1          DISABLE  30    NORMAL    TRUE
gi0/2          DISABLE  30    NORMAL    TRUE

```

#On Device1, configure the layer-2 Ethernet interface gigabitethernet0/1 as layer-3 Ethernet interface.

```

Device1(config)#interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#no switchport

#Enable the loopback detection function on the layer-3 Ethernet interface gigabitethernet0/1 of Device1
Device1(config-if-gigabitethernet0/1)#loopback-detection enable
Device1(config-if-gigabitethernet0/1)#exit

```

Step 3: Check the result.

#On Device1, view the loopback detection status.

After a loop is detected:

```

Device1#show loopback-detection
-----
Global loopback-detection : ENABLE
-----
Interface      Loopback Time(s) State      Control
-----
gi0/1          ENABLE   30    ERR-DISABLE TRUE
gi0/2          DISABLE  30    NORMAL    TRUE

```

#After Device1 detects a loop, the layer-3 Ethernet interface gigabitethernet0/1 performs close operation, and the following prompt messages are output on the device.

```

Jul 31 2014 11:29:30: %LOOP-BACK-DETECTED : loop-back send packet on gigabitethernet0/1, detected from
gigabitethernet0/1
Jul 31 2014 11:29:30: %LINEPROTO-5-UPDOWN : gigabitethernet0/1 link-status changed to err-disable
Jul 31 2014 11:29:30: %LINK-INTERFACE_DOWN-3: Interface gigabitethernet0/1, changed state to down.
Jul 31 2014 11:29:30: %LINK-LINEPROTO_DOWN-3: Line protocol on interface gigabitethernet0/1, changed state to down.

```

#Check the status of layer-3 Ethernet interface gigabitethernet0/1 on Device1. The status of layer-3 Ethernet interface becomes err-disabled.

```

Device1#show interface gigabitethernet 0/1 status err-disabled

Interface      Status      Reason
-----
gi0/1          err-disabled loopback-detect

```

### 34.3.2 Configure Local Loopback Detection

#### Network Requirements

- Device1 and Device2 form a loop through two links, and all the ports in the loop is in one VLAN.
- On Device1, loopback detection has been enabled.

- After Device1 detects a loop, it closes the interconnected layer-2 port to eliminate the loop.

### Network Topology

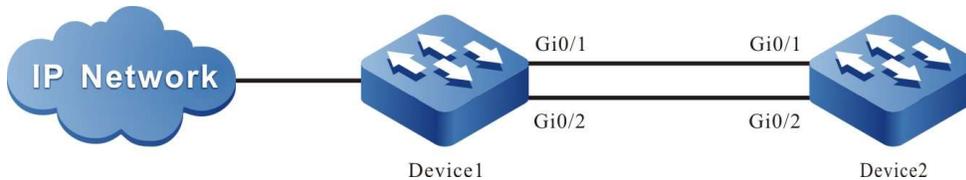


Figure 34 Network Topology for Configuration of Local Port Loopback Detection Function

### Layer-2 Ethernet interface configuration steps

Step 1: Configure the link type of VLAN and layer-2 Ethernet interface.

#Create VLAN2 on Device1.

```
Device1#configure terminal
Device1(config)#vlan 2
Device1(config-vlan2)#exit
```

#Configure the link type of layer-2 Ethernet interfaces gigabitethernet0/1 and gigabitethernet0/2 on Device1 as Trunk, allowing the services of VLAN2 to pass.

```
Device1(config)# interface gigabitethernet 0/1-0/2
Device1(config-if-range)#switchport mode trunk
Device1(config-if-range)#switchport trunk allowed vlan add 2
Device1(config-if-range)#exit
```

#Create VLAN2 on Device2.

```
Device2#configure terminal
Device2(config)#vlan 2
Device2(config-vlan2)#exit
```

#Configure the link type of layer-2 Ethernet interfaces gigabitethernet0/1 and gigabitethernet0/2 as Trunk, allowing the services of VLAN2 to pass and closing the spanning tree.

```
Device2(config)# interface gigabitethernet 0/1-0/2
Device2(config-if-range)#switchport mode trunk
Device2(config-if-range)#no switchport trunk allowed vlan 1
Device2(config-if-range)#switchport trunk allowed vlan add 2
Device2(config-if-range)#no spanning-tree enable
Device2(config-if-range)#exit
```

Step 2: Enable the loopback detection function.

#On Device1, globally enable the loopback detection function.

```
Device1(config)#loopback-detection enable
```

#On Device1, view the loopback detection status.

```
Device1#show loopback-detection
```

```
-----  
Global loopback-detection : ENABLE  
-----
```

Interface	Loopback	Time(s)	State	Control
gi0/1	DISABLE	30	NORMAL	TRUE
gi0/2	DISABLE	30	NORMAL	TRUE

#Enable the loopback detection function on the layer-2 Ethernet interface gigabitethernet0/1 of Device1.

```
Device1(config)#interface gigabitethernet 0/1  
Device1(config-if-gigabitethernet0/1)#loopback-detection enable  
Device1(config-if-gigabitethernet0/1)#exit
```

Step 3: Check the result.

#On Device1, view the loopback detection status.

After a loop is detected:

```
Device1#show loopback-detection
```

```
-----  
Global loopback-detection : ENABLE  
-----
```

Interface	Loopback	Time(s)	State	Control
gi0/1	ENABLE	30	ERR-DISABLE	TRUE
gi0/2	DISABLE	30	NORMAL	TRUE

#After Device1 detects a loop, the layer-2 Ethernet interface gigabitethernet0/1 performs close operation, and the following prompt messages are output on the device.

```
Jul 30 2014 03:29:59: %LOOP-BACK-DETECTED : loop-back send tag packet in vlan2 on gigabitethernet0/1, detected in vlan2  
from gigabitethernet0/2  
Jul 30 2014 03:29:59: %LINK-INTERFACE_DOWN-4: interface gigabitethernet0/1, changed state to down  
Jul 30 2014 03:29:59: %LINEPROTO-5-UPDOWN : gigabitethernet0/1 link-status changed to err-disable
```

#Check the status of layer-2 Ethernet interface gigabitethernet0/1 on Device1. The link status of layer-2 Ethernet interface gigabitethernet0/1 becomes Down.

```
Device1#show interface gigabitethernet 0/1  
gigabitethernet0/1 configuration information
```

```
Description      :  
Status           : Enabled  
Link             : Down (Err-disabled)  
Set Speed        : Auto  
Act Speed        : Unknown  
Set Duplex       : Auto  
Act Duplex       : Unknown  
Set Flow Control : Off  
Act Flow Control : Off  
Mdix             : Auto  
Mtu              : 1824  
Port mode        : LAN  
Port ability     : 10M HD,10M FD,100M HD,100M FD,1000M FD  
Link Delay       : No Delay  
Storm Control    : Unicast Disabled  
Storm Control    : Broadcast Disabled  
Storm Control    : Multicast Disabled  
Storm Action     : None  
Port Type        : Nni  
Pvid             : 1  
Set Medium       : Copper  
Act Medium       : Copper  
Mac Address      : 0000.0000.008b
```

---

 **Caution**

- When gigabitethernet 0/1 or gigabitethernet 0/2 of Device1 is a layer-3 Ethernet interface, there is no loop in the networking environment.
-

# 35 Error-Disable Management

---

## 35.1 Overview

The Error-Disable function is an error detection and fault recovery mechanism on ports.

Exceptions on ports may degrade the performance of the entire network or bring down the entire network. The Error-Disable function can limit the abnormality within a single device or part of the network, preventing the abnormality from affecting other normal ports and preventing the abnormality from spreading.

If an exception is detected on an open port, the port is automatically closed so that the port will not forward packets. That is, if an error condition is triggered on the port, the port is automatically disabled. This is called the Error-Disable management function, and the port status is called the Error-Disabled status.

Currently, the following functions are supported: storm suppression, port security, link flapping, DHCP rate limit, BPDU Guard, ARP detection, L2 protocol tunnel, loopback detection, OAM, and Monitor Link.

If an exception is detected on a port through the above functions, the port is automatically closed, and it is set to the Error-Disabled status. However, this status cannot continue. After the fault is eliminated, the port needs to be enabled again, and the Error-Disabled status of the port needs to be cleared so that the port can continue to forward packets. Here the automatic recovery mechanism of the Error-Disable management function is involved.

## 35.2 Error-Disable Management Function Configuration

Table 35 Error-disable Management Function Configuration List

Configuration Task	
Configure Error-Disable basic functions.	Configure Error-Disable error detection.
	Configure Error-Disable automatic recovery.

Configuration Task	
Configure Error-Disable automatic recovery.	Configure the interval for Error-Disable automatic discovery.

### 35.2.1 Configure Error-Disable Basic Functions

#### Configuration Condition

None

#### Configure Error-Disable error detection.

After the Error-Disable detection of the specification function is configured, if an exception is detected on the port, the system automatically close the port and set the port to the Error-Disabled status.

Table 35 Configuring Error-disable Error Detection

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure Error-Disable error detection.	<b>errdisable detect cause { all   bpduguard   dai   dhcp-snooping   fabric-failure   monitor-link   storm-control   link-flap   l2pt   oam   port-security   loopback-detect   ulfd   transceiver-power-high   transceiver-power-low }</b>	Mandatory  By default, all the listed functions allowed to close the port and set it as Error-Disabled.

### 35.2.2 Configure Error-Disable automatic recovery.

#### Configure Error-Disable automatic recovery.

The Error-Disable error detection mechanism enables specified functions to close a port. To quickly recover the port so that it can continue to forward packets, an automatic recovery mechanism is provided. With the mechanism, the port is automatically re-enabled after a specified interval.

Table 35 Configuring Automatic Recovery of Error-disable

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure Error-Disable automatic recovery.	<b>errdisable recovery cause</b> { <b>all</b>   <b>bpdguard</b>   <b>dai</b>   <b>dhcp-snooping</b>   <b>eips-udld</b>   <b>l2pt</b>   <b>link-flap</b>   <b>loopback-detect</b>   <b>oam</b>   <b>port-security</b>   <b>storm-control</b>   <b>transceiver-power-high</b>   <b>transceiver-power-low</b>   <b>ulfd</b> }	Mandatory  By default, a port cannot be automatically enabled, and the Error-Disabled status set by the listed functions cannot be automatically cleared. However, by default, a port can be automatically enabled and the Error-Disabled status can be automatically cleared if its status is set by the Link-Flap function.

### Configure the interval for Error-Disable automatic discovery.

You can configure the interval for a port to automatically recover normal after it port is closed by the Error-Disable error detection mechanism.

Table 35 Configuring Time Interval for Automatic Discovery of Error-disable

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the interval for Error-Disable automatic discovery.	<b>errdisable recovery interval</b> <i>interval-value</i>	Mandatory  By default, the interval at which a port is enabled and its Error-Disabled status is cleared is 300 seconds.

### 35.2.3 Error-Disable Management Monitoring and Maintaining

Table 35 Error-disable Management Monitoring and Maintaining

Command	Description
<b>show errdisable detect</b>	Displays whether it is allowed that all the listed functions close a port and set the port to the Error-Disabled status.
<b>show errdisable recovery</b>	Displays whether a port can be automatically enabled, and whether the Error-Disabled status set by the listed functions can be cleared automatically.
<b>show { interface <i>interface-list</i>   interface link-aggregation <i>link-aggregation-id</i> } status err-disabled</b>	Displays the information about Error-Disabled status setting of a specified port or aggregation group.

## 35.3 Typical Configuration Example of Error-Disable Management

### 35.3.1 Combination of Error-Disable and Storm Suppression

#### Network Requirements

- PC accesses IP Network through Device. On Device, the storm suppression and Error-Disable functions have been enabled.
- If a port of a device receives a large number of broadcast packets and then disabled, Error-Disable can re-enable the port according to the policy.

#### Network Topology



Figure 35 Network Topology for Combination of Error-disable and Storm Suppression

#### Configuration Steps

*Step 1:* Configure the link type of VLAN and port.

# Create VLAN2 on Device.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the link type of port gigabitethernet0/1 of the Device as Access, allowing the services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode access
Device(config-if-gigabitethernet0/1)#switchport access vlan 2
Device(config-if-gigabitethernet0/1)#exit
```

*Step*  
2:                   Configure the storm suppression function

#Enable the storm suppression function on port gigabitethernet0/1 of the Device, and adopt the pps limitation mode to suppress broadcast packets. The suppression rate is 200pps. When a storm occurs, the port is shutdown.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#storm-control action shutdown
Device(config-if-gigabitethernet0/1)#storm-control broadcast pps 200
Device(config-if-gigabitethernet0/1)#exit
```

*Step*  
3:                   Configure Error-disable function.

#Enable the storm suppression recovery function in Error-disable, and configure the recovery time as 30 seconds.

```
Device(config)#errdisable recovery cause storm-control
Device(config)#errdisable recovery interval 30
```

*Step*  
4:                   Check the result.

#View related configurations of Error-disable.

```
Device#show errdisable recovery

Error disable auto recovery config
interval:30 seconds
ErrDisable Reason  Timer Status
-----
bpduguard          Disabled
dai                 Disabled
dhcp-snooping      Disabled
eips-udld          Disabled
l2pt               Disabled
link-flap          Enabled
loopback-detect    Disabled
oam                Disabled
port-security      Disabled
storm-control      Enabled
ulfd               Disabled
transceiver-power-low Disabled
transceiver-power-high Disabled
```

#When the PC sends plenty of broadcast packets, the port gigabitethernet0/1 will be closed and the following prompt messages will be printed.

```
Apr 22 2021 14:40:05: %STORM_CONTROL-3: A storm detected on interface gigabitethernet0/1, ActionType:shutdown, StormType: broadcast storm
Apr 22 2021 14:40:05: %PORTMGR-LINEPROTO_DOWN-3: Line protocol on interface gigabitethernet0/1, changed state to down
```

#View the status of port gigabitethernet0/1.

```
Device#show interface gigabitethernet 0/1

gigabitethernet0/1 configuration information
  Description      :
  Status           : Enabled
  Link             : Down (Err-disabled)
  Set Speed        : Auto
  Act Speed        : Unknown
  Def Speed        : Auto
  Set Duplex       : Auto
  Act Duplex       : Unknown
  Def Duplex       : Auto
  Set Flow Control : Off
  Act Flow Control : Off
  Mdx              : Auto
  Mtu              : 1824
  Port mode        : LAN
  Port ability     : 10M FD,100M FD,1000M FD
  Link Delay       : No Delay
  Storm Control    : Unicast Pps 3000
  Storm Control    : Broadcast Pps 200
  Storm Control    : Multicast Pps 3000
  Storm Action     : Shutdown
  Port Type        : Nni
  Pvid             : 2
  Set Medium       : Copper
  Act Medium       : Copper
  Single-fiber     : Disable
  EEE              : Disable
  Mac Address      : 0001.7a54.5ca5
```

#After 30 seconds, the port gigabitethernet0/1 will be enabled, and the following prompt messages will be printed.

```
Apr 22 2021 14:40:35: %PORTMGR-AUTO_RECOVERY-5: auto recovery timer expired on interface gigabitethernet0/1, module: STROM CONTROL ACTION.
Apr 22 2021 14:40:36: %PORTMGR-LINEPROTO_UP-5: Line protocol on interface gigabitethernet0/1, changed state to up.
```

#View the status of port gigabitethernet0/1.

```
Device#show interface gigabitethernet 0/1

gigabitethernet0/1 configuration information
  Description      :
  Status           : Enabled
  Link             : Up
  Set Speed        : Auto
  Act Speed        : 1000
  Def Speed        : Auto
  Set Duplex       : Auto
  Act Duplex       : Full
  Def Duplex       : Auto
  Set Flow Control : Off
  Act Flow Control : Off
  Mdx              : Auto
  Mtu              : 1824
  Port mode        : LAN
  Port ability     : 10M FD, 100M FD,1000M FD
```

Link Delay : No Delay  
Storm Control : Unicast Pps 3000  
Storm Control : Broadcast Pps 200  
Storm Control : Multicast Pps 3000  
Storm Action : Shutdown  
Port Type : Nni  
Pvid : 2  
Set Medium : Copper  
Act Medium : Copper  
Single-fiber : Disable  
EEE : Disable  
Mac Address : 0001.7a54.5ca5

# 36 GVRP

---

## 36.1 Overview

GVRP (GARP VLAN Registration protocol) is an application protocol defined by GARP. It dynamically maintains the VLAN information in the switch based on the GARP protocol mechanism. All switches that support GVRP features can receive VLAN registration information from other switches and dynamically update local VLAN registration information, including current VLAN on the switch and which ports are included in these VLANs. Besides, these switches that support GVRP features can spread local VLAN registration information to other switches so that the VLAN configurations of all devices supporting GVRP features in the same switching network are consistent in interoperability. The VLAN registration information spread through GVRP includes both local static VLAN information manually configured and dynamic VLAN information from other switches. It should be noted that the Leave message of GVRP cannot eliminate the local VLAN manually configured as it has a higher priority than GVRP operation.

GVRP realizes the dynamic registration, maintenance and cancellation of VLAN port member information. If there is no VLAN, a VLAN will be dynamically created; if the number of VLAN port members is 0, the VLAN will be dynamically deleted, i.e. the port will be dynamically added to the VLAN or deleted from the VLAN, realizing dynamic configuration of the VLAN on the switch.

GVRP can dynamically configure VLANs so that it's unnecessary to configure all VLANs of all devices. Instead, only some devices, especially edge devices, and some special VLANs are configured. Other devices will be automatically configured through GVRP. Nowadays, enterprises always have a large network and many VLANs. The GVRP function greatly reduces the workload of administrators in configuration, as well as the possibility of manual errors. Besides, it can automatically configure VLANs when the network topology changes to ensure the connectivity between VLANs.

## 36.2 GVRP function configuration

Table 36 GVRP Function Configuration List

Configuration Task	
Enable GVRP function	Globally enable the GVRP function

Configuration Task	
Configure GVRP port	Configure the port as trunk and the VLAN allowed to pass
	Configure the port to enable GVRP function
	Configure GVRP mode for the port

### 36.2.1 Enable GVRP function

**Configuration Condition:**

None

**Globally enable GVRP function**

Globally enable GVRP function through configuration.

Table 36 Globally Enabling GVRP Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure gvrp enable	<b>gvrp enable</b>	Mandatory

### 36.2.2 Configure GVRP port

**Configuration Condition:**

None

**Configure GVRP port**

Add configuration on the port where GVRP needs to be enabled, including GVRP mode and the VLAN allowed to pass.

Table 36 Enabling GVRP Function for a Port

Step	Command	Description
Enter the global configuration mode.	configure terminal	-

Step	Command	Description
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Configure the port as trunk	switchport mode trunk	Mandatory
Allow the port to allow all VLANs	switchport trunk allowed vlan all	Mandatory
Configure the port to enable GVRP	gvrp enable	Mandatory

# 37 MLAG

---

## 37.1 Overview

MLAG is a mechanism which achieves cross-device link aggregation. It combines one device with two other paired devices for cross-device link aggregation to form a dual-active system.

As a weakly correlated horizontal virtualization technology, MLAG has the following advantages in addition to increasing bandwidth, providing link reliability, and load sharing:

- Higher reliability: MLAG improves the link reliability from single-board level to device level. For common cross-board link aggregation, if one board fails, the entire aggregation link can still work normally; for MLAG cross-device link aggregation, if one device fails, the entire aggregation link can still work normally.
- Simplified networking: MLAG, as a horizontal virtualization technology, logically virtualizes two paired devices that are double-homed into one device. MLAG provides a layer-2 topology without loops and realizes redundant backup. Therefore, the access side doesn't need spanning tree protocol, which greatly simplifies the process of networking and configuration.
- Independent upgrading: Two paired devices can be upgraded separately to ensure that one device is working normally. This has no impact on the ongoing business.

Definitions of MLAG-related concepts:

- MLAG (Multi-Chassis Link Aggregation Group) domain: Composed of two MLAG partner nodes, it forms a dual-active system.
- MLAG partner nodes: For the MLAG partner nodes, one serves as \MASTER),and the other as SLAVE.
- Peer-Link: A direct aggregation link between MLAG partner nodes, used to exchange MLAG protocol packets and transmit some data traffic.
- Keepalive: Keepalive detection between MLAG partner nodes, performed through L3 link. It determines whether one of the MLAG partner nodes is still alive when the Peer-Link fails.
- PTS (Peer-Link Transport Server): A reliable packet transmission service based on Peer-Link.
- DHD (Double-Homed Device): A device (or server) which is double-homed to the MLAG dual-active system. DHD itself may be a MLAG dual-active system.
- SD (Single-Homed Device): A device (or server) that is single-homed to the MLAG dual-

active system.

- MLAG-Port: The cross-device aggregation group between DHD and MLAG dual-active system.
- MLAG Member Port: The member port in the cross-device aggregation group between DHD and MLAG dual-active system.
- Orphan-Port: The single-homed port on the MLAG partner nodes, including the single-homed aggregation group. Orphan-Port may or may not belong to MLAG-VLAN.
- MLAG-VLAN: The VLAN where Peer-Link is added. Generally, the VLAN to which MLAG port belongs should be added into MLAG-VLAN.
- Non-MLAG-VLAN: The VLAN that doesn't contain Peer-Link. Generally, non-MLAG-VLAN doesn't contain MLAG port.
- MLAG-VLANIF: VLANIF interface corresponding to MLAG-VLAN.
- Non-MLAG-VLANIF: VLANIF interface corresponding to non-MLAG-VLAN.
- Unpaired: After the Peer-Link port is disconnected, if the Keepalive is normal, it is believed that an Unpaired failure has occurred. This will cause the MLAG port and MLAG-VLANIF on the SLAVE node to Suspend so that the uplink and downlink traffic is forwarded through the MASTER node.
- Up-Delay: When the MLAG partner nodes restart or Peer-Link failure recovers, the MLAG port will be set as UP after a period of delay.
- Auto-Recovery: After a period of time, when the MLAG node of local port believes that it is completely disconnected from the MLAG node of peer port (as a matter of fact, the MLAG node of peer port may have device failure or still be alive), MLAG node of local port deems itself as the only node and becomes a master node to forward traffic.
- Dual-Master: If both Peer-Link and Keepalive fail, when the SLAVE node believes that it is completely disconnected from the MASTER node, the SLAVE node will be upgraded to a MASTER node, and the original MASTER node still exists. Then, there are two MASTER nodes, i.e. Dual-Master. There may be abnormal traffic forwarding in Dual-Master state.
- Control protocol packet (also called PEERING packet): The protocol packet exchanged between MLAG nodes, used for node pairing, role election, etc. It is sent and received via UDP.
- Data synchronization packet (also called SYNC packet): The synchronization packet exchanged between MLAG nodes, used for transmission of control information of each service, relay service protocol packet, synchronization service entries, etc. It is sent and received via TCP after the SYNC packet encapsulates the PTS header.
- Control VLAN: The layer-3 VLAN (interface vlan) used to transmit PTS synchronization

packets. Only Peer-Link can be added into this VLAN. Other ports cannot be added into this VLAN.

- Suspend: Here it means shutdown, i.e. the shutdown of MLAG aggregation group or MLAG-VLANIF interface.

## 37.2 MLAG function configuration

Table 37 MLAG Function Configuration List

Configuration Task	
Create MLAG domain	Create MLAG domain
Configure MLAG parameters	Configure the automatic recovery delay time after the node is restarted
	Configure MLAG node ID
	Configure the role priority of MLAG node
	Configure preemption mode
	Configure the MAC address of MLAG system
	Configure the priority of MLAG system
	Configure the delay time and interval time of UP state
Configure Keepalive parameters	Configure the source and destination addresses of Keepalive packet
	Set the sending interval and receiving timeout of Keepalive packet
	Set the silent period of Keepalive

Configure Peer-Link	Configure the layer-2 aggregation interface as a Peer-Link port
Configure MLAG port	Configure MLAG port
Configure Orphan-Port	Configure the Orphan-Port of the SLAVE node to be set as shutdown when the Peer-Link fails but the Keepalive is normal

---

 **Note**

- MLAG function, supporting software learning instead of hardware learning
- 

### 37.2.1 Create MLAG domain

In MLAG partner nodes, the MLAG domain ID must be consistent.

#### Configuration Condition

Before creating MLAG domain, ensure that:

- On the MLAG partner nodes, there are no other MLAG domains.

#### Create MLAG domain

Create MLAG domain.

Table 37 Creating MLAG Domain

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Create MLAG domain	<b>mlag domain <i>domain-id</i></b>	Mandatory  By default, no MLAG domain is created, and the value range of domain ID is 1~255.

## 37.2.2 Configure MLAG parameters

### Configuration Condition

Before configuring MLAG parameters, ensure that:

- Create MLAG domain.

### Configure the automatic recovery delay time after the node is restarted

After the device is started, start the automatic recovery timer with the configured automatic recovery delay time. If no Keepalive or Peering packet is received until the timer times out, and the Peer-Link is always Down, it is believed that there is no peer node, and this node becomes the MASTER.

Table 37 Configuring Automatic Recovery Delay Time After Restarting of Node

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the MLAG domain configuration mode	<b>mlag domain</b> <i>domain-id</i>	-
Configure the automatic recovery delay time after the node is restarted	<b>auto-recovery reload-delay</b> <i>delay_value</i>	Optional By default, the automatic recovery delay time is 240 seconds. It ranges from 240 to 3600 seconds.

### Configure MLAG node ID

In the same MLAG domain, the MLAG node IDs are different and unique.

Table 37 Configuring MLAG Node ID

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Enter the MLAG domain configuration mode	<b>mlag domain</b> <i>domain-id</i>	-
Configure MLAG node ID	<b>node id</b> <i>id-number</i>	Mandatory  By default, no MLAG node ID is configured. Its range is 1 and 2.

### Configure the role priority of MLAG node

The node role priority is used for master-slave role election between two nodes in the same MLAG domain. The smaller the value, the higher the priority. The one with a higher priority becomes the Master device. If the nodes have the same priority, compare the bridge MAC addresses of the two devices. The one with a smaller bridge MAC address becomes the Master device.

Table 37 Configuring MLAG Node Role Priority

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the MLAG domain configuration mode	<b>mlag domain</b> <i>domain-id</i>	-
Configure the role priority of MLAG node	<b>node role-priority</b> <i>priority-value</i>	Optional  By default, the MLAG node priority is 100. Its range is 1~ 254.

### Configure preemption mode

If the preemption mode is configured, when the master-slave role is elected, the previous role of the node will be ignored. The node role will be determined according to the node priority and the MAC comparison result: the lower the node priority value, the higher the priority, and the one with higher priority becomes the Master device; if the nodes have the same priority, compare the bridge MAC addresses of the two devices (the one with a smaller bridge MAC address becomes the Master device).

Table 37 Configuring Preemption Mode

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the MLAG domain configuration mode	<b>mlag domain</b> <i>domain-id</i>	-
Configure preemption mode	<b>role preempt</b>	Optional By default, no preemption mode is configured.

### Configure the MAC address of MLAG system

In order to enable the access device to deem the two nodes in MLAG domain as one device, the MAC addresses of the MLAG system of the two nodes must be the same.

Table 37 Configuring MAC Address of MLAG System

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the MLAG domain configuration mode	<b>mlag domain</b> <i>domain-id</i>	-
Configure the MAC address of MLAG system	<b>system-mac</b> <i>mac_address</i>	Optional By default, the MAC address of MLAG system is not configured. The MAC addresses of MLAG systems of the two nodes are the same and automatically generated according to the domain id.

### Configure the priority of MLAG system

In order to enable the access device to deem the two nodes in MLAG domain as one device, the MLAG system priority of the two nodes must be the same.

Table 37 Configuring MLAG System Priority

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the MLAG domain configuration mode	<b>m lag domain</b> <i>domain-id</i>	-
Configure the priority of MLAG system	<b>system-priority</b> <i>priority_value</i>	Optional By default, the MLAG system priority is 32768. Its range is 1~65535.

#### Configure the delay time and interval time of UP state

When the device is added into the MLAG domain as a SLAVE node, the MLAG interface will be set as UP state after the period of UP state delay. During the period of UP state delay, the MAC address table, ARP table and other information must be synchronized. Therefore, if there are many entries, the local timer can be properly extended to avoid packet loss.

Table 37 Configuring Delay Time and Interval Time of UP State

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the MLAG domain configuration mode	m lag domain domain-id	-
Configure the delay time and interval time of UP state	up-delay delay_seconds [interval interval_mseconds]	Optional By default, the delay time and interval time of UP state are 90 seconds and 1000 milliseconds, and they range from 1 to 3600

		seconds and from 1 to 300000 milliseconds respectively.
--	--	---

### Configure MLAG graceful restart

After graceful restart is enabled, the local node will notify the peer node to delay the keep-alive time of control protocol and Keepalive. This can avoid traffic interruption due to the timeout of peer node when the MLAG of local node is restarted. It is recommended that this command be configured only before MLAG is restarted. Under normal conditions, configuring this command will make the peer node insensitive to network changes.

By default, MLAG graceful restart is disabled.

Table 37 Configuring MLAG Graceful Restart

Step	Command	Description
Enter the privilege configuration mode	<b>enable</b>	-
Configure MLAG graceful restart and the keep-alive time of peer port control protocol and Keepalive after the restart	<b>mlag graceful-restart [holding-time seconds ]</b>	- Optional By default, the keep-alive time is 300 seconds. Its range is 200-20000 seconds.

### Configure reserved interface

Configure the VLAN interface of the SLAVE node to be set as shutdown when the Peer-Link fails but the Keepalive is normal.

By default, no reserved interface is configured.

Table 37 Configuring Reserved Interface

Step	Command	Description
Enter the interface configuration mode	<b>interface vlan [vlan-id]</b>	-
Configure reserved interface	<b>mlag unpaired reserved</b>	Optional The vlan corresponding to the interface must be MLAG-VLAN. This

		command is not required for non-MLAG-VLANIF interface as it will not be configured as shutdown.
--	--	---

### 37.2.3 Configure Keepalive parameters

#### Configuration Condition

Before configuring Keepalive parameters, ensure that:

- Create MLAG domain.

#### Configure the source and destination addresses of Keepalive packet

To enable the MLAG system to be correctly established, the source and destination addresses of Keepalive packets must be configured, and it is reachable between two nodes at layer 3.

The VLAN corresponding to the layer-3 interface where the source IP address of Keepalive packet belongs shall not be included in the VLAN of Peer-Link port.

Table 37 Configuring Source and Destination Addresses of Keepalive Packet

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the MLAG domain configuration mode	mlag domain domain-id	-
Configure the source and destination addresses of Keepalive packet	keepalive ip destination ipv4_address source ipv4_address [udp-port udp-number] [vrf vrf_name]	Mandatory By default, udp-port is 53910, VRF name global, and udp-port range 1~65535. VRF name supports 31 characters at most.

#### Configure the sending interval and receiving timeout of Keepalive packet

After the Keepalive receiving timeout timer is enabled, if the next Keepalive packet is not received before this timer expires, it is deemed LOST.

Table 1 Configuring Sending Interval and Receiving Timeout of Keepalive Packet

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the MLAG domain configuration mode	mlag domain domain-id	-
Configure the sending interval and receiving timeout of Keepalive packet	keepalive interval mseconds [timeout seconds]	Optional By default, the sending interval and receiving timeout of Keepalive packet are 1000 milliseconds and 6s, and they range from 100 to 10000 milliseconds and from 1 to 20 seconds respectively.

### Configure the silent period of Keepalive

After the Peer-Link link becomes DOWN, the SLAVE node enters the silent period. The Keepalive packets received during the silent period will be ignored and will not be processed until the silent period expires. The silent period can be set to allow the Keepalive packets on the link to be received and sent completely so as to avoid false detection caused by packet delay.

Table 37 Configuring Keepalive Silent Period

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the MLAG domain configuration mode	mlag domain domain-id	-
Configure the silent period of Keepalive	keepalive quiet-time mseconds	Optional By default, the Keepalive silent period is 3000 milliseconds. Its

		range is 1~15000 milliseconds.
--	--	--------------------------------

### 37.2.4 Configure Peer-Link

#### Configuration Condition

Before configuring Peer-Link, ensure that:

- Create MLAG domain.

#### Configure the layer-2 aggregation interface as a Peer-Link port

As a direct aggregation link between two MLAG devices, Peer-Link can be used to exchange MLAG protocol packets and transmit some data traffic.

Table 2 Configuring Layer-2 Aggregation Interface as a Peer-Link Port

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the layer-2 aggregation interface configuration mode	interface link-aggregation link-aggregation-id	-
Configure the layer-2 aggregation interface as a Peer-Link port	mlag peer-link	Mandatory By default, no Peer-Link port is configured.

### 37.2.5 Configure MLAG port

#### Configuration Condition

Before configuring MLAG port, ensure that:

- Create MLAG domain.

#### Configure MLAG port

In order to improve reliability and avoid loops in the process of configuration, on the two MLAG partner nodes, configure the same MLAG port ID for the aggregation groups that are connected to the same aggregation group on the DHD to form a cross-device link aggregation group.

Table 3 Configuring MLAG Port

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the layer-2 aggregation interface configuration mode	interface link-aggregation link-aggregation-id	-
Configure MLAG port	mlag group mlag-id	Mandatory  By default, no MLAG port is configured. The MLAG port ID ranges from 1 to 1000.

---

### Note

- It is recommended that the link aggregation group be configured as a dynamic aggregation group.
- 

## 37.2.6 Configure Orphan-Port

### Configuration Condition

Before configuring Orphan-Port, ensure that:

- Create MLAG domain.

### Configure the Orphan-Port of the SLAVE node to be set as shutdown when the Peer-Link fails but the Keepalive is normal

By default, when the Peer-Link fails but the Keepalive is normal, all the MLAG ports of the SLAVE node will be configured as shutdown, but the Orphan-Port will not be configured as such state. To configure some Orphan-Ports as shutdown, this command needs to be configured for these ports.

Table 13-7 Configuring the Mode of Orphan-Port of SLAVE Node as Shutdown When the Peer-Link Fails but the Keepalive Is Normal

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Layer-2 Ethernet interface configuration mode	interface interface-name	At least one option must be selected.
Enter the layer-2 aggregation interface configuration mode	interface link-aggregation link-aggregation-id	After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on current port. After you enter the layer-2 aggregation interface configuration mode, the subsequent configuration takes effect only within current aggregation group.
Configure the Orphan-Port of the SLAVE node to be set as shutdown when the Peer-Link fails but the Keepalive is normal	m lag unpaired orphan-port suspend	Optional By default, this command is not configured.

### 37.2.7 MLAG monitoring and maintaining

Table 4 MLAG Monitoring and Maintaining

Command	Description
<b>clear mlag packet keepalive statistics [tx   rx]</b>	Clear statistical information of MLAG Keepalive packets

Command	Description
<b>clear mlag packet peering statistics [tx   rx]</b>	Clear statistical information of MLAG Peering packets
<b>clear mlag packet pts statistics [application <i>app-id</i>] [tx   rx]</b>	Clear statistical information of MLAG PTS packets
<b>clear mlag packet sync statistics [tx   rx]</b>	Clear statistical information of MLAG Sync packets
<b>show mlag pts application</b>	Show information of all MLAG services
<b>show mlag brief</b>	Show summary information of MLAG
<b>show mlag group [<i>mlag-id</i>]</b>	Show information of MLAG aggregation group
<b>show mlag keepalive</b>	Show information of MLAG Keepalive
<b>show mlag node</b>	Show information of MLAG node
<b>show mlag packet pts [application [<i>app-id</i>]] statistics</b>	Show statistical information of PTS packets sending and receiving of MLAG's all services or specified services
<b>show mlag packet keepalive statistics</b>	Show statistical information of MLAG Keepalive packets
<b>show mlag packet peering statistics</b>	Show statistical information of MLAG paired packets
<b>show mlag packet sync statistics</b>	Show statistical information of MLAG synchronous packets
<b>show mlag suspend</b>	Show the Suspended interface
<b>show mlag up-delay</b>	Show the interface waiting for timeout of up-delay timer

## 37.3 Typical MLAG configuration example

### 37.3.1 Configure basic functions of MLAG

#### Network Requirements

- All devices are within the same layer-2 network.

#### Network Topology

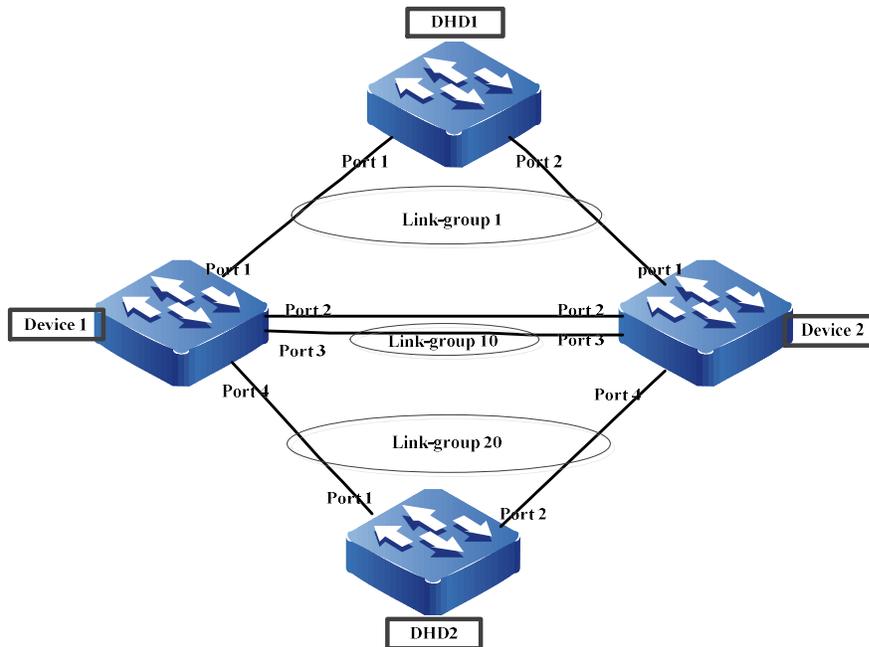


Figure 37 Configuring Basic Functions of MLAG

#### Configuration Steps

Step 1: Add the interface into the aggregation group and vlan. (The addition of interface into the aggregation group is omitted)

#Configure Device1. Add the interface into the peerlink aggregation group, peerlink aggregation into vlan, and keepalive port into vlan.

```
Device1#configure terminal
Device1(config)#vlan 2-4094
Please wait .....
Done.
Device1(config)# link-aggregation 10 mode lacp
Device1(config)# interface port3
Device1(config-if-port3)# link-aggregation 10 active
Device1(config-if-port3)#exit
Device1(config)# interface link-aggregation 10
Device1(config-link-aggregation10)# switchport mode trunk
Device1(config-link-aggregation10)# switchport trunk allowed vlan add 2-4093
Device1(config-link-aggregation10)# no switchport trunk allowed vlan 1
Device1(config-link-aggregation10)# switchport trunk pvid vlan 2
Device1(config-link-aggregation10)#exit
```

```
Device1(config)# interface port2
Device1(config-if-port2)# switchport access vlan 4094
Device1(config-if-port2)#exit
```

#Configure Device2. Add the interface into the peerlink aggregation group, peerlink aggregation into vlan, and keepalive port into vlan.

```
Device2#configure terminal
Device2 (config)#vlan 2-4094
Please wait .....
Done.
Device2 (config)# link-aggregation 10 mode lacp
Device2 (config)# interface port3
Device2 (config-if-port3)# link-aggregation 10 active
Device2 (config-if-port3)#exit
Device2 (config)# interface link-aggregation 10
Device2 (config-link-aggregation10)# switchport mode trunk
Device2 (config-link-aggregation10)# switchport trunk allowed vlan add 2-4093
Device2 (config-link-aggregation10)# no switchport trunk allowed vlan 1
Device2 (config-link-aggregation10)# switchport trunk pvid vlan 2
Device2 (config-link-aggregation10)#exit
Device2 (config)# interface port2
Device2 (config-if-port2)# switchport access vlan 4094
Device2 (config-if-port2)#exit
```

Step 2: Configure MLAG domain.

#Configure Device1. Configure MLAG domain instance.

```
Device1#configure terminal
Device1(config)#mlag domain 1
Device1(config-mlag-domain)#node id 1

Device1(config-mlag-domain)#keepalive ip destination 30.0.0.10 source 30.0.0.20
Device1(config-mlag-domain)#exit
```

#Configure Device2. Configure MLAG domain instance.

```
Device2#configure terminal
Device2(config)#mlag domain 1
Device2(config-mlag-domain)#node id 2
Device2(config-mlag-domain)#keepalive ip destination 30.0.0.20 source 30.0.0.10
Device2(config-mlag-domain)#exit
```

**Note:**

The domain IDs of the two MLAG nodes must be the same;

The node IDs of the two MLAG nodes must be different;

Step 3: Configure the keepalive ip interface.

#Configure Device1. Configure keepalive ip interface.

```
Device1(config)#interface vlan 4094
Device1(config-if-vlan4094)#ip address 30.0.0.20 24
Device1(config-if-vlan4094)#exit
Device1(config)#
```

#### #Configure Device2. Configure keepalive ip interface.

```
Device2(config)#interface vlan 4094
Device2(config-if-vlan4094)#ip address 30.0.0.10 24
Device2(config-if-vlan4094)#exit
Device2(config)#
```

#### Step 4: Configure MLAG group and peer-link group.

##### #Configure Device1. Configure MLAG group and peer-link group.

```
Device1(config)#interface link-aggregation 1
Device1(config-link-aggregation1)#mlag group 1
Device1(config-link-aggregation1)#exit
Device1(config)#
Device1(config)# interface link-aggregation 10
Device1(config-link-aggregation10)#mlag peer-link
Device1(config-link-aggregation10)#exit
Device1(config)#
Device1(config)# interface link-aggregation 20
Device1(config-link-aggregation20)#mlag group 20
Device1(config-link-aggregation20)#exit
Device1(config)#
```

##### #Configure Device2. Configure MLAG group and peer-link group.

```
Device2(config)# interface link-aggregation 1
Device2(config-link-aggregation1)#mlag group 1
Device2(config-link-aggregation1)#exit
Device2(config)#
Device2(config)# interface link-aggregation 10
Device2(config-link-aggregation10)#mlag peer-link
Device2(config-link-aggregation10)#exit
Device2(config)#
Device2(config)# interface link-aggregation 20
Device2(config-link-aggregation20)#mlag group 20
Device2(config-link-aggregation20)#exit
Device2(config)#
```

#### #View the MLAG information on Device1

```
Device1#sho mlag brief
MLAG domain id      : 1
Role FSM status     : SLAVE
Peering FSM status  : ESTABLISHED
Keepalive FSM status : ALIVE
PTS Service         : ON
Up-delay            : 90sec
Graceful-restart    : Disabled
Number of mlags configured : 2
```

```
-----
Peer-Link      Link-status Data-status Active-vlans
-----
```

link-aggregation 10 UP UP 2-4093

-----  
Node ID Role System-MAC System-Priority  
-----

Self 1 SLAVE 0001.7a95.000b 32768  
Remote 2 MASTER 0001.7a95.000b 32768

Device1#

Device1#show mlag group

Number of mlags configured : 2

mlag-id: 1 (link-aggregation1)

--Link status: UP

--Data status: UP

--Active mlag vlans: 2-4093

--Redirect FSM state: UNREDIRECT

--Isolate FSM state: ISOLATE

--Block FSM state: UNBLOCK

--Remote interface: link-aggregation 1

--Remote link status: UP

--Remote data status: UP

mlag-id: 20 (link-aggregation 20)

--Link status: UP

--Data status: UP

--Active mlag vlans: 2-4093

--Redirect FSM state: UNREDIRECT

--Isolate FSM state: ISOLATE

--Block FSM state: UNBLOCK

--Remote interface: link-aggregation 20

--Remote link status: UP

--Remote data status: UP

Device1#

### 37.3.2 Configure multi-level MLAG functions

#### Network Requirements

- Deploy a multi-level MLAG environment to create a loop-free network. This environment supports dual-homing access to ensure reliability, and the link supports load to improve link utilization.

#### Network Topology

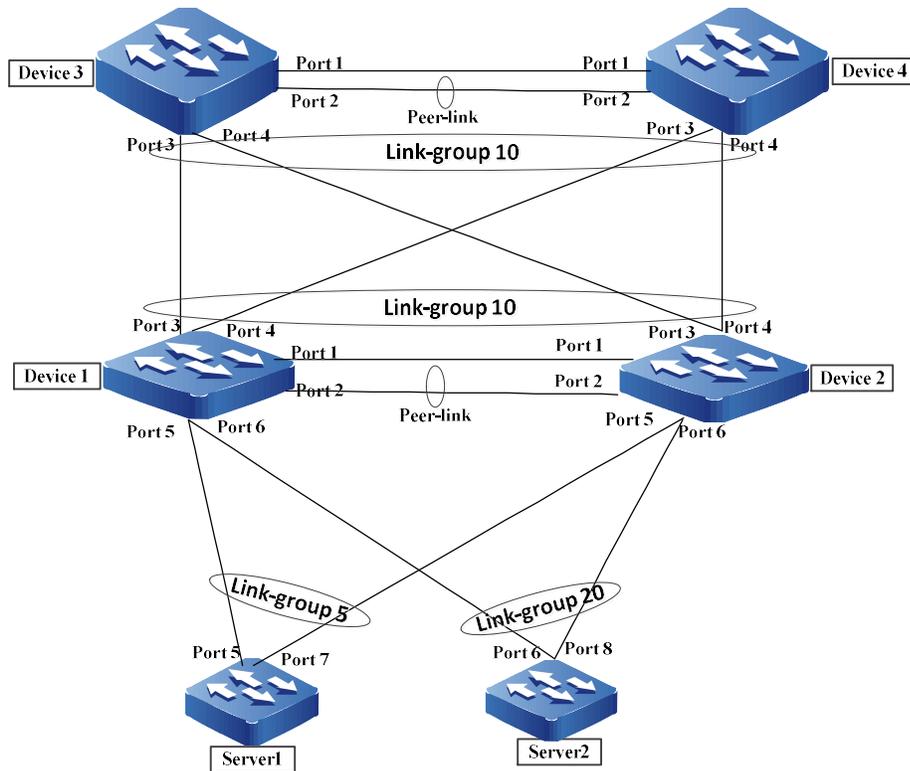


Figure 37 Configuring Level-2 MLAG Functions

#### Configuration idea:

1. MLAG is configured between the aggregation and access switches Device1 and Device2 and between Device3 and Device4 for dual-homing access. Any device failure has no impact on services, which can ensure high service reliability.
2. Aggregation switches Device3 and Device4 are root bridge devices. Root protection is configured on their downlinks to protect the normal forwarding of traffic. The interface which connects the access switches Device1 and Device2 with the terminal is configured with edge ports to ensure network convergence time, and BPDU protection function is configured to improve the stability of network.

3. Aggregation switches Device3 and Device4 are configured with vlan interface and vrrp to make a dual-active gateway.

### Configuration Steps

#### Step 1: Add the port connected to the access device and server into link aggregation

#Configure Device1

Device1#configure terminal

Device1(config)# link-aggregation 5 mode lacp

Device1(config)# link-aggregation 20 mode lacp

Device1(config)# interface port5

Device1(config-if-port5)# link-aggregation 5 active

Device1(config)# interface port6

Device1(config-if-port6)# link-aggregation 20 active

#Configure Device2

Device2#configure terminal

Device2(config)# link-aggregation 5 mode lacp

Device2(config)# link-aggregation 20 mode lacp

Device2(config)# interface port5

Device2(config-if-port5)# link-aggregation 5 active

Device2(config)# interface port6

Device2(config-if-port6)# link-aggregation 20 active

#### Step 2: Configure mstp for Device1, Device2, Device3 and Device4

#Configure the MST domain of Device1, with domain name mlag and version number 1, and activate it.

Device1#configure terminal

Device1(config)#spanning-tree mst configuration

Device1(config-mst)#region-name admin

Device1(config-mst)#revision-level 1

Device1(config-mst)#active configuration pending

Device1(config-mst)#exit

---

 **Note**

The MST domain configuration of Device2, Device3, and Device 4 is the same as that of Device1. (Omitted)

---

#The specified priority of Device3 is 0.

Device3(config)#spanning-tree pseudo-information

Device3 (config-stp-pseudo)#mst instance 0 designated-priority 0

#Enable BA function on the inline port of Device1 & Device2, Device3 & Device4

Device1(config)#interface link-aggregation 1

Device1(config-link-aggregation1)# spanning-tree bridge-assurance enable

Device2(config)#interface link-aggregation 1

Device2(config-link-aggregation1)# spanning-tree bridge-assurance enable

Device3(config)#interface link-aggregation 1

Device3(config-link-aggregation1)# spanning-tree bridge-assurance enable

Device4(config)#interface link-aggregation 1

Device4(config-link-aggregation1)# spanning-tree bridge-assurance enable

#Globally enable spanning tree for Device1 & Device2, Device3 & Device4

Device1(config)# spanning-tree enable

Device2(config)# spanning-tree enable

Device3(config)# spanning-tree enable

Device4(config)# spanning-tree enable

### **Step 3: Configure mlag domain, peer-link, mlag group, and mlag interface**

Device1#configure terminal

Device1(config)# link-aggregation 1 mode lacp

Device1(config)# link-aggregation 10 mode lacp

Device1(config)# interface port2

Device1(config-if-port2)# link-aggregation 1 active

Device1(config)# interface port1

Device1(config-if-port1)# switchport access vlan 10

```
Device1(config)# interface port1,3
Device1 (config-if-range)# link-aggregation 10 active
#Configure mlag domain
Device1#configure terminal
Device1(config)#mlag domain 1
Device1(config-mlag-domain)#node id 1
Device1(config-mlag-domain)#keepalive ip destination 12.1.1.2 source 12.1.1.1
Device1(config-mlag-domain)#exit
#Configure peer-link and mlag group
Device1(config)#interface link-aggregation 1
Device1(config-link-aggregation1)# mlag peer-link
Device1(config-link-aggregation1)#exit
Device1(config)# interface link-aggregation 5
Device1(config-link-aggregation5)# mlag group 5
Device1(config-link-aggregation5)#exit
Device1(config)# interface link-aggregation 10
Device1(config-link-aggregation10)# mlag group 10
Device1(config-link-aggregation10)#exit
Device1(config)# interface link-aggregation 20
Device1(config-link-aggregation20)#mlag group 20
Device1(config-link-aggregation20)#exit
#Configure keepalive interface address
Device1(config)#interface vlan 10
Device1(config-if-vlan10)#ip address 12.1.1.1 24
Device1(config-if-vlan10)#exit
Device1(config)# interface link-aggregation 1
Device1(config-link-aggregation1)# switchport mode trunk
Device1(config-link-aggregation1)# switchport trunk allowed vlan add 20,30,40
Device1(config-link-aggregation1)# exit
```

```
Device1(config)# interface link-aggregation 5
Device1(config-link-aggregation5)# switchport mode trunk
Device1(config-link-aggregation5)# switchport trunk allowed vlan add 20,30,40
Device1(config-link-aggregation5)# exit
Device1(config)# interface link-aggregation 10
Device1(config-link-aggregation10)# switchport mode trunk
Device1(config-link-aggregation10)# switchport trunk allowed vlan add 20,30,40
Device1(config-link-aggregation10)# exit
Device1(config)# interface link-aggregation 20
Device1(config-link-aggregation20)# switchport mode trunk
Device1(config-link-aggregation20)# switchport trunk allowed vlan add 20,30,40
Device1(config-link-aggregation20)# exit
```

---

 **Note**

The configuration of Device2 is the same as that of Device1, except for the following:

---

```
#Configure mlag domain
Device2#configure terminal
Device2(config)#mlag domain 1
Device2(config-mlag-domain)#node id 2
Device2(config-mlag-domain)#keepalive ip destination 12.1.1.1 source 12.1.1.2
Device2(config-mlag-domain)#exit
#Configure keepalive interface address
Device2(config)#interface vlan 10
Device2(config-if-vlan10)#ip address 12.1.1.2 24
Device2(config-if-vlan10)#exit
#Configure Device3
Device3#configure terminal
```

```
Device3(config)# link-aggregation 1 mode lacp
Device3(config)# interface port2
Device3(config-if-port2)# link-aggregation 1 active
Device3(config)# interface port1
Device3(config-if-port1)# switchport access vlan 100
Configure mlag domain
Device3#configure terminal
Device3(config)#mlag domain 255
Device3(config-mlag-domain)#node id 1
Device3(config-mlag-domain)#keepalive ip destination 34.1.1.4 source 34.1.1.3
Device3(config-mlag-domain)#exit
Configure peer-link and mlag groups
Device3(config)#interface link-aggregation 1
Device3(config-link-aggregation1)# mlag peer-link
Device3(config-link-aggregation1)#exit
Device3(config)# interface link-aggregation 10
Device3(config-link-aggregation10)# mlag group 10
Device3(config-link-aggregation10)#exit
#Configure keepalive interface address
Device3(config)#interface vlan 100
Device3(config-if-vlan100)#ip address 34.1.1.3 24
Device3(config-if-vlan100)#exit
Device3(config)# interface link-aggregation 1
Device3(config-link-aggregation1)# switchport mode trunk
Device3(config-link-aggregation1)# switchport trunk allowed vlan add 20,30,40
Device3(config-link-aggregation1)# exit
Device3(config)# interface link-aggregation 10
Device3(config-link-aggregation10)# switchport mode trunk
Device3(config-link-aggregation10)# switchport trunk allowed vlan add 20,30,40
```

Device3(config-link-aggregation10)# exit

---

 **Note**

The configuration of Device4 is the same as that of Device3, except for the following:

---

Device4#configure terminal

Device4(config)#mlog domain 255

Device4(config-mlog-domain)#node id 2

Device4(config-mlog-domain)#keepalive ip destination 34.1.1.3 source 34.1.1.4

Device4(config-mlog-domain)#exit

Device4(config)#interface vlan 100

Device4(config-if-vlan100)#ip address 34.1.1.4 24

Device4(config-if-vlan100)#exit

**Step 4: Configure static vrrp**

Device3(config)# interface vlan 20

Device3 (config-if-vlan20)# ip address 20.0.0.1 24

Device3 (config-if-vlan20)#vrrp 1 ip 20.0.0.254

Device3 (config-if-vlan20)# vrrp 1 static

Device3 (config-if-vlan20)#exit

Device3(config)# interface vlan 30

Device3 (config-if-vlan30)# ip address 30.0.0.1 24

Device3 (config-if-vlan30)#vrrp 1 ip 30.0.0.254

Device3 (config-if-vlan30)# vrrp 1 static

Device3 (config-if-vlan30)#exit

Device3(config)# interface vlan 40

Device3 (config-if-vlan40)# ip address 40.0.0.1 24

Device3 (config-if-vlan40)#vrrp 1 ip 40.0.0.254

Device3 (config-if-vlan40)# vrrp 1 static

Device3 (config-if-vlan40)#exit

```

Device4(config)# interface vlan 20
Device4 (config-if-vlan20)# ip address 20.0.0.2 24
Device4 (config-if-vlan20)#vrrp 1 ip 20.0.0.254
Device4 (config-if-vlan20)# vrrp 1 static
Device4(config-if-vlan20)#exit
Device4(config)# interface vlan 30
Device4 (config-if-vlan30)# ip address 30.0.0.2 24
Device4 (config-if-vlan30)#vrrp 1 ip 30.0.0.254
Device4(config-if-vlan30)# vrrp 1 static
Device4 (config-if-vlan30)#exit
Device4(config)# interface vlan 40
Device4(config-if-vlan40)# ip address 40.0.0.2 24
Device4 (config-if-vlan40)#vrrp 1 ip 40.0.0.254
Device4 (config-if-vlan40)# vrrp 1 static
Device4 (config-if-vlan40)#exit

```

**Step 5: View the verification result**

#View the MLAG information on Device1

```
Device1#sho mlag brief
```

```
MLAG domain id      : 1
```

```
Role FSM status    : MASTER
```

```
Peering FSM status : ESTABLISHED
```

```
Keepalive FSM status : ALIVE
```

```
PTS Service       : ON
```

```
Up-delay         : 90sec
```

```
Graceful-restart  : Disabled
```

```
Number of mlags configured : 2
```

```
-----
Peer-Link      Link-status Data-status Active-vlans
```

```
-----  
link-aggregation 1  UP  UP    20,30,40
```

```
-----  
Node  ID  Role  System-MAC  System-Priority  
-----
```

```
Self  1  SLAVE 0001.7a98.000b 32768
```

```
Remote 2  MASTER 0001.7a98.000b 32768
```

```
Device1#show mlag group
```

```
Number of mlags configured : 2
```

```
mlag-id: 5 (link-aggregation5)
```

```
--Link status: UP
```

```
--Data status: UP
```

```
--Active mlag vlans: 20,30,40
```

```
--Redirect FSM state: UNREDIRECT
```

```
--Isolate FSM state: ISOLATE
```

```
--Block FSM state: UNBLOCK
```

```
--Remote interface: link-aggregation 5
```

```
--Remote link status: UP
```

```
--Remote data status: UP
```

```
mlag-id: 20 (link-aggregation 20)
```

```
--Link status: UP
```

```
--Data status: UP
```

```
--Active mlag vlans: 20,30,40
```

```
--Redirect FSM state: UNREDIRECT
```

```
--Isolate FSM state: ISOLATE
```

```
--Block FSM state: UNBLOCK
```

--Remote interface: link-aggregation 20

--Remote link status: UP

--Remote data status: UP

#View the MLAG information on Device3

Device3#sho mlag brief

MLAG domain id : 1

Role FSM status : MASTER

Peering FSM status : ESTABLISHED

Keepalive FSM status : ALIVE

PTS Service : ON

Up-delay : 90sec

Graceful-restart : Disabled

Number of mlags configured : 2

-----  
Peer-Link      Link-status Data-status Active-vlans  
-----

link-aggregation 1    UP    UP      20,30,40

-----  
Node ID Role System-MAC System-Priority  
-----

Self 1 SLAVE 0001.7a95.000b 32768

Remote 2 MASTER 0001.7a95.000b 32768

Device3#show mlag group

Number of mlags configured : 1

mlag-id: 10 (link-aggregation10)

--Link status: UP

--Data status: UP  
--Active mlag vlans: 20,30,40  
--Redirect FSM state: UNREDIRECT  
--Isolate FSM state: ISOLATE  
--Block FSM state: UNBLOCK  
--Remote interface: link-aggregation 5  
--Remote link status: UP  
--Remote data status: UP

Device3##sho spanning-tree mst

Spanning-tree enabled protocol mstp

MST Instance 00 vlans mapped: 1-4094

Bridge address 0001.7a95.000b priority 0

Region root address 0001.7a95.000b priority 0

Designated root address 0001.7a95.000b priority 0

root: 0, rpc: 0, epc: 0, hop: 20

We are the root of the spanning tree

Operational hello time 2, forward time 15, max age 20, message age 0

Configured hello time 2, forward time 15, max age 20, max hops 20, hold count 6

Flap guard : admin false, max count 5, detect period 10s, recovery period 30s

Tc protection: admin true, threshold 1, interval 4s, rxTcCnt 0, status:NORMAL

ARL flush: enabled,logPortState: disabled

Bpdu length-check: false, bpdu illegal length packets count: 0

Autoedge swap-check: true

Swap-delay time: 30

Configured timer factor: 3

Topology Change Count:0, last change occurred:0 hour 0 minute 0 second(0 seconds)

Interface	Role	Sts	Cost	Prio.Nbr	Type
-----------	------	-----	------	----------	------

```

-----
link-agg10    Desg FWD 18000    128.1182 P2P (MLAG 10)
link-agg1    Desg FWD 19500    128.1280 P2P (MLAG peer-link)

```

Device1#sho spanning-tree mst

Spanning-tree enabled protocol mstp

MST Instance 00 vlans mapped: 1-4094

Bridge address 0001.7a98.000b priority 0

Region root address 0001.7a95.000b priority 0

Designated root address 0001.7a95.000b priority 0

root: 34846, rpc: 18000, epc: 0, hop: 19

Operational hello time 2, forward time 15, max age 20, message age 0

Configured hello time 2, forward time 15, max age 20, max hops 20, hold count 6

Flap guard : admin false, max count 5, detect period 10s, recovery period 30s

Tc protection: admin true, threshold 1, interval 4s, rxTcCnt 0, status:NORMAL

ARL flush: enabled,logPortState: disabled

Bpdu length-check: false, bpdu illegal length packets count: 0

Autoedge swap-check: true

Swap-delay time: 30

Configured timer factor: 3

Topology Change Count:0, last change occurred:0 hour 0 minute 0 second(0 seconds)

```

Interface      Role Sts Cost    Prio.Nbr Type
-----
link-agg5      Desg FWD 19500    128.0082 P2P (MLAG 5)
link-agg10     Desg FWD 19500    128.0096 P2P (MLAG 20)
link-agg1      Desg FWD 490      128.0144 P2P (MLAG peer-link)

```

# 38 VLAN Isolation

## 38.1 Overview

In the users' access network, in order to realize mutual isolation between different user groups, different user groups need to be divided into different VLANs. When users in the same user group intend to be isolated from other users, they can use the port isolation technology. But if this technology is used, the administrator needs to know the location of the port of the users' access network. It will lead to inconvenient configuration, management and maintenance. VLAN isolation technology can solve this problem. The administrator simply needs to configure VLAN isolation for the VLAN where the user group is located. Then, users in the user group are isolated from each other. By configuring the uplink port of VLAN isolation, users in the user group can access public network through the uplink port. This technology provides a safer and more flexible solution for networking.

## 38.2 VLAN isolation function configuration

Table 38 VLAN Global Function Configuration List

Configuration Task	
Configure VLAN isolation	Enable the VLAN isolation function
	Configure the uplink port of VLAN isolation

### 38.2.1 Configure VLAN isolation

#### Configuration Condition

None

#### Enable the VLAN isolation function

By enabling the VLAN isolation function, you can realize mutual isolation between the member ports in VLAN.

Table 38 Enabling Global VLAN Isolation

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the VLAN configuration mode	<b>vlan <i>vlan-id</i></b>	-
Enable the VLAN isolation function	<b>vlanisolat enable</b>	Mandatory  By default, the VLAN isolation function is disabled.

### Configure the uplink port of VLAN isolation

After the uplink ports of VLAN isolation are configured, the downlink ports in the VLAN are still isolated from each other. However, intercommunications between uplink ports and downlink ports are possible.

Table 38 Configuring Uplink Port of VLAN Global Isolation

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface <i>interface-name</i></b>	-
Configure the uplink port of VLAN global isolation	<b>vlanisolate uplink-port vlan <i>vlan-id</i></b>	Mandatory  By default, no uplink port of VLAN isolation is configured.

### Note

- After the VLAN global isolation function is disabled, the configured uplink port of VLAN isolation is automatically cancelled, VLAN isolation is enabled, and all ports in the VLAN

---

are downlink ports by default.

---

### 38.2.2 VLAN isolation monitoring and maintaining

Table 38 VLAN Global Isolation Monitoring and Maintaining

Command	Description
<b>show vlan-isolate( [ vlan <i>vlan-id</i> ])</b>	Show the information of VLAN isolation

# 39 ARP

---

## 39.1 Overview

Address Resolution Protocol (ARP) provides dynamic mapping from IP addresses to MAC addresses. The Ethernet frames to be transmitted in the Ethernet can be encapsulated properly only after MAC addresses are specified. The ARP protocol is used to obtain MAC addresses that correspond to IP addresses.

## 39.2 ARP Function Configuration

Table 39-1 ARP Function Configuration List

Configuration Task	
Configure Basic Functions of ARP	Configure static ARP
	Configure local ARP advertisement

Configuration Task	
	Configure the maximum number of dynamic ARP entries
	Configure the dynamic ARP aging time
	Enable dynamic ARP learning
	Enable Dynamic ARP Learning
	Configure ARP Receive Queue Depth
	Configure ARP Proxy
	Enable ARP fast response

### 39.2.1 Configure Basic Functions of ARP

#### Configuration Condition

None

#### Configure static ARP

Configuring static ARP means that the user manually specifies the mapping relationship between IP addresses and MAC addresses.

Table 39-2 Configuring Static ARP

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure static ARP	<b>arp [ vrf vrf-name ] { ip-address   host-name } mac-address [ alias [ advertise ]   advertise [ alias ] ] [ vlan vlan-id ] [ interface if-name ]  </b>	Mandatory

Step	Command	Description
	{ <b>link-aggregation</b> <i>link-aggregation-id</i> }}	

## Note

- When the configured static ARP entry contains an alias option, if an ARP request for this IP address is received, the MAC address in the static ARP entry is used for response.
- When the configured static ARP entry contains an advertise option, the static ARP will be regularly advertised when the static ARP advertisement is enabled.
- When static ARP is bound to a specific port or aggregation group, the static ARP takes effect only on that port or aggregation group.

### Configure local ARP advertisement

ARP request packets are broadcast packets. When there are a large number of ARP requests in the network, it is easy to cause a broadcast storm in the network, which can result in normal ARP request packets being overwhelmed and ARP unable to be learned. In this case, you can reduce the possibility of broadcast storms by configuring the local ARP advertisement feature to reduce ARP requests.

Table 39-3 Configuring Local ARP Advertisement

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure local ARP advertisement	<b>arp local-announce enable</b>	Mandatory
Configure local ARP advertisement interval.	<b>arp local-announce interval</b> <i>seconds</i>	Optional The default value is 10 seconds.
Configure local ARP advertisement rate.	<b>arp local-announce rate</b> <i>speed</i>	Optional

Step	Command	Description
		The default value is 1 packet per second.

### Configure the maximum number of dynamic ARP entries

The maximum number of dynamic ARP entries is configured to avoid dynamically learned ARP from taking up too many system resources.

Table 39-4 Configuring the Maximum Number of Dynamic ARP Entries

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the maximum number of dynamic ARP entries	<b>arp limited</b> <i>max-entries</i>	Mandatory The default maximum number of entries is 8000.

### Configure the dynamic ARP aging time

There is a survival period, or aging time, for dynamically learned ARPs. During the aging time, the device will send ARP requests periodically, reset the aging time if an ARP response is received, and delete the dynamic ARP table entry when the aging time expires.

Table 39-5 Configuring Dynamic ARP Aging Time

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure the dynamic ARP aging time	<b>arp timeout</b> { <i>second</i> / <b>disable</b> }	Mandatory

Step	Command	Description
		The default aging time is 1200 seconds.

### Enable Dynamic ARP Learning

By default, a dynamic ARP learning is enabled on a device. To prevent dynamic learning from occupying too many system resources, you can disable the dynamic ARP learning function. After dynamic ARP learning is disabled, after the local device receives an ARP request for the MAC address of the local device, it sends an ARP response but does not generate any related ARP entry. An ARP entry is generated only when the local device requests for the MAC address of a peer device.

Table 39-6 Enabling Dynamic ARP Learning

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable Dynamic ARP Learning	<b>arp learn-active</b>	Mandatory  By default, the dynamic ARP passive learning function is enabled.

### Enables Interface Dynamic ARP Learning

An interface can perform dynamic ARP learning by default. To increase reliability and security, users can disable the interface dynamic ARP learning function and use static ARP, which can effectively prevent ARP spoofing.

Table 39-7 Enabling Dynamic ARP Learning Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-

Step	Command	Description
Enable dynamic ARP learning	<b>arp dynamic-learn</b>	Mandatory By default, the dynamic ARP learning function is enabled.

### Configure ARP Receive Queue Depth

The ARP packets received by the device will be first cached to the ARP receive queue. The system will read the packets from the queue in order and then handle the packets. When the cached ARP packets reach the queue depth, the subsequently received APR packets will be dropped. The user can adjust the ARP receive queue depth based on the network ARP emergency.

Table 39-8 Configuring ARP Packet Receive Queue Depth

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure ARP Receive Queue Depth	<b>arp queue-length <i>length</i></b>	Mandatory The default ARP packet receive queue depth is 200.

### Configure ARP Proxy

An ARP request is sent by the host of one network to another network, and the intermediate device between the two networks can respond to the ARP request. This process is called ARP proxy.

Table 39-9 Configuring ARP Proxy

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure ARP Proxy	<b>ip proxy-arp</b>	Mandatory By default, the ARP proxy function is enabled.

### Configure ARP Fast Response

By default, after receiving the ARP packets, the device will send the packets to the MPU to learn and respond. After enabling the ARP fast response function, the device can give fast responses to the packets in the LPU.

Table 39-10 Configuring ARP Fast Response

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure ARP Fast Response	<b>arp fast-response</b>	Mandatory By default, the global ARP fast response function is disabled.

## 39.2.2 ARP monitoring and maintaining

Table 39-11 ARP Monitoring and Maintaining

Command	Description
<b>show arp</b> [ <i>vrf vrf-name</i> ]	View ARP table
<b>show arp attack-detection</b>	View information about suspected hosts of ARP attacks
<b>show arp statistic</b>	View ARP statistics

## 39.3 Typical Configuration Example of ARP

### 39.3.1 Configure ARP Proxy

#### Network Requirements

- Device is directly connected to PC1 and PC2 respectively. The network number of the LAN where PC1 and PC2 are located is the same, both are 10.0.0.0/16.
- The MAC address of Device's interface VLAN2 is 0001.7a13.0102.
- Through the ARP proxy of Device, PC1 is able to ping through to PC2, and PC1 can learn the MAC address of PC2.

#### Network Topology

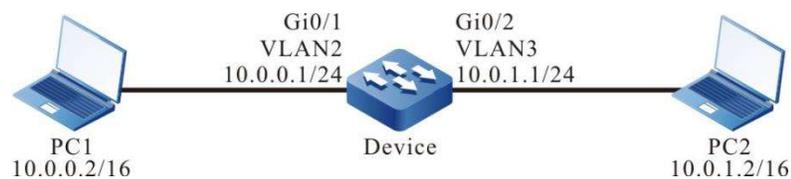


Figure 39-1 Network Topology for Configuring ARP Proxy

#### Configuration Steps

- Step 1: Configure Virtual Local Area Networks (VLANs), and add ports to the required VLANs. (Omitted)
- Step 2: Configure IP addresses for the ports. (Omitted)
- Step 3: Check the result.

# PC1 ping PC2 at the address 10.0.1.2.

```
C:\Documents and Settings>ping 10.0.1.2

Pinging 10.0.1.2 with 32 bytes of data:

Reply from 10.0.1.2: bytes=32 time<1ms TTL=255

Ping statistics for 10.0.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

# View Device's ARP table entries.

```
Device#show arp
Protocol Address   Age (min) Hardware Addr  Type   Interface  Swithport
Internet 10.0.0.1   -    0001.7a13.0102 ARPA   vlan2     ---
Internet 10.0.0.2   1    B8AC.6F2D.4498 ARPA   vlan2     gigabitethernet0/1
Internet 10.0.1.1   -    0001.7a13.0103 ARPA   vlan3     ---
Internet 10.0.1.2   1    4437.e603.0d63 ARPA   vlan3     gigabitethernet0/2
```

# View the ARP table entries of PC1.

```
C:\Documents and Settings>arp -a

Interface: 10.0.0.2 --- 0x5
Internet Address      Physical Address   Type
10.0.0.1              00-01-7a-13-01-02 dynamic
10.0.1.2              00-01-7a-13-01-02 dynamic
```

# PC1 is able to ping through to PC2, and PC1 can learn the MAC address of PC2.

---

## Note

- The device has ARP proxy enabled by default.
- 

## 39.3.2 Configure static ARP

### Network Requirements

- Device is directly connected to the PC.
- The MAC address of the PC is 4437.e603.0d63.
- Bind the IP address and MAC address of PC on Device.
- PC is able to ping through to the address of the interface VLAN2 of Device.

### Network Topology

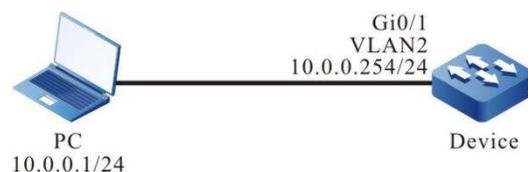


Figure 39-2 Network Topology for Configuring Static ARP

### Configuration Steps

Step 1: Configure VLAN, and add ports to the corresponding VLAN. (Omitted)

Step 2: Configure IP addresses for the ports. (Omitted)

Step 3: Bind the IP address and MAC address of PC on Device.

#Configure Device.

Bind the IP address and MAC address of PC to Device.

```
Device(config)#arp 10.0.0.1 4437.e603.0d63
```

Step 4: Check the result.

# View Device's ARP table entries.

```
Device1#show arp
Protocol Address Age (min) Hardware Addr Type Interface Switchport
Internet 10.0.0.1 - 4437.e603.0d63 ARPA vlan2 gigabitethernet0/1
Internet 10.0.0.254 - 0001.7a13.0102 ARPA vlan2 ---
```

#The PC is able to ping through to the address of the interface VLAN2 of Device 10.0.0.254.

```
C:\Documents and Settings>ping 10.0.0.254

Pinging 10.0.0.254 with 32 bytes of data:

Reply from 10.0.0.254: bytes=32 time<1ms TTL=255

Ping statistics for 10.0.0.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

#The PC is able to ping through to the address of the interface VLAN2 of Device 10.0.0.254.

# 40 IP Basics

---

## 40.1 Overview

The Internet Protocol (IP) is based on data packets. It is used in data exchange between computer networks. The protocols that are supported by the device include: IP, Internet Control Message Protocol (ICMP), Transfer Control Protocol (TCP), User Datagram Protocol (UDP), and Socket.

Among them, IP packets are the base of the TCP/IP protocol stack. The IP layer is responsible for addressing, fragmentation, reassembly, and protocol information partitioning. As the network layer protocol, the IP protocol performs route addressing and control packet transmission.

The UDP protocol and the TCP protocol is set up based on the IP protocol. They provide connection-based reliable data transmission services and non-connection-based unreliable data transmission services respectively.

ICMP is mainly used to provide network detection services. It also provides an error report if the network layer or transmission layer protocol becomes abnormal, and it informs the related device of the abnormality to facilitate network control management.

## 40.2 IP Basic Function Configuration

Table 40-1 IP Basic Function Configuration List

Configuration Task	
Configure an IP address.	Configure an IP address for an interface.
	Configure an unnumbered IP address for an interface.
Configure basic functions of the IP protocol.	Configure the depth of the IP packet receiving queue.
	Configure the Time To Live (TTL) of transmitted IP packets.

Configuration Task	
	Configure timeout for packet reassembly.
	Enable IP packet receiving verification and check.
	Configure transmitted IP packets to calculate a checksum.
	Enable IP routing cache.
Configure basic functions of the ICMP protocol.	Enable global ICMP redirection.
	Enable global ICMP redirection.
	Enable ICMP destination unreachable.
	Configure ICMP rate limit.
Configure basic functions of the TCP protocol.	Configure the size of the TCP receiving cache.
	Configure the size of the TCP transmitting cache.
	Configure the maximum number of TCP retransmissions.
	Configure the maximum length of TCP packets.
	Configure the maximum TCP round-trip time.
	Configure the TCP connection idle time.
	Configure TCP connection setup waiting time.
	Configure the maximum number of TCP keep-alive times.
	Enable the TCP timestamp.
Enable TCP selective retransmission.	
Configure basic functions of the UDP protocol.	Configure TTL of UDP packets.
	Configure the size of the UDP receiving cache.
	Configure the size of the UDP transmitting cache.

Configuration Task	
	Enable UDP verification and check.
	Fill in UDP packet checksum.

### 40.2.1 Configure an IP address.

An IP address is a 32-bit number which uniquely identifies a network device that runs the IP protocol on the Internet.

An IP address consists of the following two parts:

- Network number (Net-id): It identifies the network in which the device is located.
- Host number (Host-id): It specifies the host number in the device network.

To facilitate IP address management, IP addresses are categorized into five classes, and each IP address class has its own functions. IP addresses of classes A to C are used for address allocation, IP addresses of class D is used in multicast applications, and IP addresses of class E are used for test purpose. The following table shows the IP addresses classes and their ranges.

Table 40-2 IP Address Classes and Their Ranges

Address Type	Available Network Address Range	Description
A	1.0.0.0 ~ 127.0.0.0	Network number 127 is used for loopback interfaces.
B	128.0.0.0 ~ 191.255.0.0	-
C	192.0.0.0 ~ 223.255.255.0	-
D	224.0.0.0 ~ 239.255.255.255	Class D addresses are used for multicast.
E	240.0.0.0 ~ 255.255.255.254	Class E addresses are used for test purpose.

With the development of the Internet, IP address resources have gradually been consumed up. Address allocation based on classes causes address waste, so the concept of "subnet" is introduced. "Subnet" takes some host numbers in the IP addresses as subnet numbers. In this way, a large network is divided into multiple subnets. This facilitates network planning and deployment.

The three address segments, 10.0.0.0-10.255.255.255, 172.16.0.0-172.16.255.255, and 192.168.0.0-192.168.255.255 are private and reserved addresses, and they cannot be allocated to the public network.

This section describes how to configure an interface IP address and how to configure an unnumbered interface IP address.

### Configuration Condition

None

### Configure an IP address for an interface.

An IP address can only be configured for an interface that supports the IP protocol. One interface can only be configured with one primary IP address but it can be configured with multiple secondary IP addresses.

Table 40-3 Configuring an IP Address for an Interface

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure an IP address for an interface.	<b>ip address</b> <i>ip-address</i> { <i>network-mask</i>   <i>mask-len</i> } [ <b>secondary</b> ]	Mandatory

---

### Note

- One interface can only be configured with one primary IP address, therefore, the newly configured primary IP address replaces the original primary IP address.
  - Before an interface is configured with secondary IP addresses, the interface must be configured a primary IP address. An interface can be configured with a maximum of 100 secondary IP addresses.
  - The IP addresses of different interfaces must not in the same network segment, but the primary and secondary IP addresses of one interface can be in the same network segment.
- 

### Configure an unnumbered IP address for an interface.

Unnumbered IP addresses save IP addresses. In the case of unnumbered IP addresses, the IP addresses of other interfaces can be borrowed instead of allocated independently. If an unnumbered interface generates an IP packet, the source IP address of the packet is the primary IP address of a borrowed

interface. In configuring an unnumbered IP address for an interface, the interface to be borrowed must be specified, so that the IP address of the interface can be borrowed.

Table 40-4 Configuring an Unnumbered IP Address for an Interface

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure an unnumbered IP address for an interface.	<b>ip unnumbered</b> <i>reference-interface</i>	Mandatory

---

### Note

- The borrowed interface must be configured with the primary IP address, and the interface must not be configured with an unnumbered IP address.
  - The primary IP address of an interface can be borrowed by multiple interfaces, but only the primary IP address of the interface can be borrowed.
- 

## 40.2.2 Configure basic functions of the IP protocol.

In the TCP/IP protocol stack, the IP protocol is the network layer core protocol that is responsible for network interconnection. The IP protocol is a connectionless protocol. Before transmitting data, you need not set up a connection. The IP protocol tries best to deliver packets, but it does not ensure that all packets can reach the destination orderly.

### Configuration Condition

None

### Configure the depth of the IP packet receiving queue.

The IP packets received by a device are first cached in the IP packet receiving queue of an interface. The system reads packets orderly in the queue for processing. If the cached IP packets reach the specified queue depth, the later IP packets are discarded. You can adjust the depth of the IP packet receiving queue according to burst of IP packets in the network.

Table 40-5 Configuring the Depth of the IP Packet Receiving Queue

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the depth of the IP packet receiving queue to a specified value.	<b>ip option queue-length</b> <i>queue-size</i>	Mandatory  By default, the depth of the IP packet receiving queue is 200.
Configure the depth of the IP packet receiving queue to the default value.	<b>default ip option queue-length</b>	Optional

### Configure the Time To Live (TTL) of transmitted IP packets.

The header of an IP packet contains the Time-To-Live (TTL) field, which is decreased by 1 once the IP packet passes a routing device. When the TTL is zero, the device discards the IP packet. By default, the TTL of IP packets transmitted by the device is 255, that is, the packet can only be transmitted for up to 255 times. If you want to limit the number of packet forwarding times, adjust the TTL value for the transmitted IP packets.

Table 40-40 Configuring the TTL of Transmitted IP Packets

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the TTL of transmitted IP packets to a specified value.	<b>ip option default-ttl</b> <i>ttl - value</i>	Mandatory  By default, the TTL of transmitted IP packets is 255.
Configure the TTL of transmitted IP packets to a default value.	<b>default ip option default-ttl</b>	Optional

### Configure timeout for packet reassembly.

If an IP packet is fragmented during the transmission, after the fragments reach the destination, they need to be reassembled to form a complete IP packet. Before all fragments are received, the received fragments

are cached temporarily. If reassembly times out before all fragments reach the destination, the received fragments are discarded.

Table 6-7 Configuring Timeout for Packet Reassembly

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configuring timeout for packet reassembly to a specified value.	<b>ip option fragment-ttl</b> <i>ttl-value</i>	Mandatory  By default, the timeout for packet reassembly is 60, and the unit is 0.5 second.
Configuring timeout for packet reassembly to the default value.	<b>default ip option fragment-ttl</b>	Optional

---

 **Note**

- The unit for timeout of packet reassembly is 0.5 second.
- 

### Enable IP Packet Receiving Verification and Check

You can enable this function to verify and check the received IP packets. If the checksum is incorrect, the packet will be discarded.

Table 40-40 Enabling IP Packet Verification and Check

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable IP packet receiving verification and check.	<b>ip option recv-checksum</b>	Mandatory  By default, the function is enabled.
Configure the method for verifying and checking the	<b>default ip option recv-checksum</b>	Optional

Step	Command	Description
received IP packets to the default value.		

**Enable IP routing cache.**

After a packet is sent from socket to the IP layer, if the destination address is the same as the previous packet and the route is valid, the packet directly use the route in the cache without the need of searching for another route.

Table 40-8 Enabling IP Routing Cache

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable IP routing cache.	<b>ip upper-cache</b>	Mandatory By default, the IP routing cache function is enabled.

**40.2.3 Configure basic functions of the ICMP protocol.**

In the TCP/IP protocol stack, ICMP is mainly used to provide network detection services. It also provides an error report if the network layer or transmission layer protocol becomes abnormal, and it informs the related device of the abnormality to facilitate network control management.

**Configuration Condition**

None

**Enable global ICMP redirection.**

After a device receives an IP packet to be forwarded, if it is found that the receiving interface of the packet and the transmitting interface of the packet are the same through route selection, the device forwards the packet and sends back an ICMP redirection packet to the source end, requesting the source end to reselect the correct next hop for transmission of later packets. By default, a device can send ICMP redirection packets. In some special cases, you can prohibit a device from sending ICMP redirection packets.

Table 40-9 Enabling Global ICMP Redirection

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable global ICMP redirection.	<b>ip redirect</b>	Mandatory By default, the global ICMP redirection function is enabled.

### Enable global ICMP redirection.

In sending ICMP redirection packets, if you need to send ICMP redirection packets, you need to enable the ICMP redirection function on the interface.

Table 40-10 Enabling Global ICMP Redirection

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Enable global ICMP redirection.	<b>ip redirects</b>	Mandatory By default, the ICMP redirection function is enabled on an interface.

### Note

- You can send ICMP redirection packets only when the ICMP redirection function is enabled globally and on the interface.

### Enable Global ICMP Destination Unreachable

After a device receives IP data packets, if the destination is unreachable, the packet is discarded and the ICMP destination unreachable error packet is sent back to the source end.

- If route selection of a forwarded IP packet fails, the network unreachable ICMP error packet is sent back to the source end.

Table 40-11 Enabling ICMP Destination Unreachable

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable ICMP Destination Unreachable	<b>ip network unreachable reply</b>	Optional By default, the ICMP destination unreachable function is disabled.

**Enable ICMP destination unreachable.**

After a device receives IP data packets, if the destination is unreachable, the packet is discarded and the ICMP destination unreachable error packet is sent back to the source end.

- If route selection of a forwarded IP packet fails, the network unreachable ICMP error packet is sent back to the source end.
- For an IP packet that can be forwarded, if you need to fragment the IP packet but a Don't Fragment (DF) bit is set in the packet, an ICMP error packet indicating that "segmentation is required but a DF bit is set" is sent to the source end.
- For an IP packet whose destination address is the local device, if the device does not support the upper-layer protocol of the device, it sends a "protocol unreachable" ICMP error packet to the source end.
- For an IP packet whose destination address is the local device, if the transport layer port of the packet of the packet does not match the port that the device process monitors, the device sends back a "port unreachable" ICMP error packet to the source end.

If a device encounters a malicious attack by a large number of ICMP destination unreachable packets, the device performance is degraded, and network traffic is increased. To prevent such case, you can disable the function of sending ICMP destination unreachable packets.

Table 40-12 Enabling ICMP Destination Unreachable

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface <i>interface-name</i></b>	-

Step	Command	Description
Enable ICMP destination unreachable.	<b>ip unreachable</b>	Optional By default, the ICMP destination unreachable function is enabled.

### Configure ICMP rate limit.

If a device encounters a malicious attack by a large number of ICMP error packets, the device performance is degraded, and network traffic is increased. To prevent such case, you can configure ICMP packet rate limit. The types of ICMP error packets include: unreachable packets, redirection packets, TTL timeout packets, and parameter error packets. The default rate limit of the packets is 10pps, while the transmitting rate of the other types of packets is 0, that is, no rate limit. In addition, you can configure the transmitting rates for different types of packets independently. If no rate is configured for a type of packets, the default value is used.

Table 40-13 Configuring ICMP Rate Limit

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable ICMP rate limit.	<b>ip icmp ratelimit enable</b>	Mandatory By default, the function is enabled.
Configure ICMP rate limit.	<b>ip icmp ratelimit</b> { <b>default</b> <i>pps</i> / <b>echo-reply</b> { <i>pps</i>   <b>unlimit</b> }   <b>mask-reply</b> { <i>pps</i>   <b>unlimit</b> }   <b>param-problem</b> { <i>pps</i>   <b>unlimit</b> }   <b>redirect</b> { <i>pps</i>   <b>unlimit</b> }   <b>time-exceed</b> { <i>pps</i>   <b>unlimit</b> }   <b>time-stamp-reply</b> { <i>pps</i>   <b>unlimit</b> }   <b>unreach</b> { <i>pps</i>   <b>unlimit</b> } }	Mandatory By default, the ICMP rate limit function is enabled.

## 40.2.4 Configure basic functions of the TCP protocol.

In the TCP/IP protocol stack, TCP is a connection-oriented transport layer protocol. Before sending data through the TCP protocol, you must first set up a connection. The TCP protocol provides congestion control and ensures reliable data transmission.

## Configuration Condition

None

### Configure the size of the TCP receiving cache.

In some special network environment, you can configure both the size of receiving cache and the size of transmitting cache of a TCP connection so that the network can reach the optimal performance. If the TCP connection receiving cache is not configured, the size of the receiving cache is the default value.

Table 40-14 Configuring the Size of the TCP Receiving Cache

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the size of the TCP receiving cache.	<b>ip tcp rcvbufs</b> <i>buff-size</i>	Mandatory By default, the size of the receiving cache is 8192 bytes.

### Configure the size of the TCP transmitting cache.

In some special network environment, you can configure both the size of receiving cache and the size of transmitting cache of a TCP connection so that the network can reach the optimal performance. If the TCP connection transmitting cache is not configured, the size of the transmitting cache is the default value.

Table 40-15 Configuring the Size of the TCP Transmitting Cache

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the size of the TCP transmitting cache.	<b>ip tcp sendbufs</b> <i>buff-size</i>	Optional By default, the size of the transmitting cache is 8192 bytes.

### Configure the maximum number of TCP retransmissions.

After the server sends a SYN-ACK packet, if it does not receive a response packet from the client, the server retransmits the packet. If the number of retransmissions exceeds the maximum number of retransmissions defined by the system, the system disconnects the TCP connection.

Table 40-16 Configuring the Maximum Number of TCP Retransmissions

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the maximum number of TCP retransmissions.	<b>ip tcp retransmits</b> <i>retransmits-count</i>	Mandatory  By default, the maximum number of TCP retransmissions is 3.

#### Configure the maximum length of TCP packets.

The maximum length of TCP packets is the maximum length of data blocks that are sent by the transmitting end of a TCP connection to the receiving end. When a connection is set up, the smaller maximum packet length of the two ends is used as the maximum packet length in sending TCP packets by the two ends. If a TCP packet exceeds the maximum packet length, the transmitting ends fragments the packet before sending it.

Table 40-17 Configuring the Maximum Length of TCP Packets

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the maximum length of TCP packets.	<b>ip tcp segment-size</b> <i>seg-size</i>	Optional  By default, the maximum length of TCP packets is 512 bytes.

#### Configure the maximum TCP round-trip time.

The TCP round trip time refers to the time between the timepoint at which the transmitting end sends a TCP packet and the timepoint at which the transmitting end receives the response packet. The maximum TCP round-trip time that is configured during TCP connection setup is taken as the initial value of the TCP round-trip time. The later TCP round-trip time is calculated according to the actual round-trip time. By default, the maximum TCP round-trip time is 3 seconds.

Table 40-18 Configuring the Maximum TCP Round-Trip Time

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the maximum TCP round-trip time.	<b>ip tcp round-trip</b> <i>round-trip-time</i>	Mandatory  By default, the maximum TCP round-trip time is 3 seconds.

**Configure the TCP connection idle time.**

After a TCP connection is set up, if no data is exchanged, the TCP connection idle time times out. Then TCP performs a keep-alive test. After the maximum number of keep-alive times is reached, the TCP connection is disconnected. By default, the TCP connection idle time is 2 hours.

Table 40-19 Configuring the TCP Connection Idle Time

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the TCP connection idle time.	<b>ip tcp idle-timeout</b> <i>idle-time</i>	Mandatory  By default, the TCP connection idle time is 14400, and the unit is 0.5 second.

---

 **Note**

- The unit of the TCP connection idle time is 0.5 second.
- 

**Configure TCP connection setup waiting time.**

The setup of a TCP connection requires three handshakes. After a TCP client sends a connection request packet, it waits for the response from the TCP server before completing connection setup. After the time

for waiting for connection setup timeout before a response is received, connection setup is terminated. By default, the time for waiting for setting up a TCP connection is 75 seconds.

Table 40-20 Configuring TCP Connection Setup Waiting Time

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure TCP connection setup waiting time.	<b>ip tcp init-timeout</b> <i>init-time</i>	Mandatory  By default, the time for waiting for setting up a TCP connection is 150 seconds, and the unit is 0.5 second.

### Note

- The unit of the TCP connection setup waiting time is 0.5 second.

### Configure the maximum number of TCP keep-alive times.

If no data is exchanged on a TCP connection for TCP connection idle time, a TCP keep-alive packet is sent for keep-alive test. If the keep-alive test fails, a keep-alive test is performed again. If the maximum number of TCP keep-alive times exceeds the threshold, the TCP connection will be disconnected. By default, the maximum number of TCP keep-alive times is 3.

Table 40-21 Configuring the Maximum Number of TCP Keep-Alive Times

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the maximum number of TCP keep-alive times.	<b>ip tcp keep-count</b> <i>keep-count</i>	Mandatory  By default, the maximum number of TCP keep-alive times is 3.

### Enable the TCP timestamp.

TCP automatically calculates the packet round-trip time according to the serial number of the request packet and that of the response packet. However, the calculation is not accurate. Use of TCP timestamps can revise the problem. The transmitting end adds a timestamp into a packet, and the receiving end sends back the timestamp in the response packet. The transmitting end calculates the packet round-trip time according to the returned timestamp. By default, the function is disabled.

Table 40-22 Enabling the TCP Timestamp

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable the TCP timestamp.	<b>ip tcp timestamp</b>	Mandatory By default, the function is disabled.

#### Enable TCP selective retransmission.

After TCP sends a series of packets, if the transmission of one packet fails, the series of packets need to be retransmitted. After TCP selective transmission is enabled, then only the packet that fails to be transmitted needs to be retransmitted. By default, the function is disabled.

Table 40-23 Enabling TCP Selective Retransmission

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure TCP selective retransmission.	<b>ip tcp selective-ack</b>	Mandatory By default, the function is disabled.

### 40.2.5 Configure TCP Protocol Anti-Attack Function

The TCP server receives a large number of SYN packets but the peer end does not respond to the SYN-ACK response from the server. This can cause the server's memory to be consumed heavily, taking up the server's syn queue and causing the TCP server unable to service normal requests. Such attacks can be avoided by configuring TCP anti-attack function.

#### Configuration Condition

None

### Enable TCP Syncache Function

This function does not rush to allocate the TCB when a SYN data packet is received, but first responds with a SYN ACK packet and stores this half-open connection information in a dedicated HASH table (Cache) until a correct response ACK packet is received before allocating the TCB.

Table 40-24 Enabling TCP Syncache Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure TCP syncache function	<b>ip tcp syncache</b>	Mandatory By default, the function is disabled.

### Enable TCP Syncookies Function

This function does not use any storage resources at all, it uses a special algorithm to generate Sequence Number. The algorithm takes into account fixed information including the other party's IP, port, its own IP and port, and other fixed information of its own, such as MSS, time, etc. After receiving the other party's ACK packet, the algorithm will recalculate it to see if it is the same as the other party's response packet (Sequence Number-1), so as to decide whether to allocate TCB resources.

Table 40-25 Enabling TCP Syncookies Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the TCP syncookies function.	<b>ip tcp syncookies</b>	Mandatory By default, the function is disabled.

## 40.2.6 Configure basic functions of the UDP protocol.

In the TCP/IP protocol stack, UDP is a connectionless-oriented transport layer protocol. Before sending data through the TCP protocol, you need not set up a connection. The UDP protocol provides unreliable data transmission without congestion control.

### Configuration Condition

User manual  
Release 1.0 01/2022

None

### Configure TTL of UDP packets.

Configuring TTL of UDP packets means to fill in the TTL value in the IP header of UDP packets. The header of an IP packet contains the Time-To-Live (TTL) field, which is decreased by 1 once the IP packet passes a routing device. When the TTL is zero, the device discards the IP packet. By default, the TTL value of the IP packet of a UDP packet is 64.

Table 40-26 Configuring TTL of UDP Packets

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure TTL of UDP packets.	<b>ip udp default-ttl</b> <i>time-to-live</i>	Mandatory By default, the TTL value of the IP packet of a UDP packet is 64.

### Configure the size of the UDP receiving cache.

In some special network environment, you can configure both the size of receiving cache and the size of transmitting cache of a UDP connection so that the network can reach the optimal performance. If the UDP connection receiving cache is not configured, the size of the receiving cache is the default value, 41600 bytes.

Table 40-278 Configuring the Size of the UDP Receiving Cache

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the size of the UDP receiving cache.	<b>ip udp recvbuffers</b> <i>buffer-size</i>	Mandatory By default, the size of the UDP receiving cache is 41600 bytes.

### Configure the size of the UDP transmitting cache.

In some special network environment, you can configure both the size of receiving cache and the size of transmitting cache of a UDP connection so that the network can reach the optimal performance. If the UDP connection transmitting cache is not configured, the size of the transmitting cache is the default value, 9216 bytes.

Table 40-28 Configuring the Size of the UDP Transmitting Cache

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the size of the UDP transmitting cache.	<b>ip udp sendbuffers</b> <i>buffer-size</i>	Mandatory  By default, the size of the UDP transmitting cache is 9216 bytes.

#### Enable UDP verification and check.

To prevent errors that occur during transmission of UDP packets, after UDP packets are received, UDP verification and check need to be performed. The system compares the UDP packet verification field calculated by the receiving end and the UDP packet header checksum field. If the two values are different, the system determines that a transmission error has occurred, and then discards the packet. By default, the function is enabled.

Table 40-29 Enabling UDP Verification and Check

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable UDP verification and check.	<b>ip udp recv-checksum</b>	Mandatory  By default, the function is enabled.

#### Fill in UDP packet checksum.

To prevent UDP packets from encountering transmission errors, in transmitting UDP packets, the transmitting end fills in the UDP packet checksum to be calculated into the UDP packet header checksum field for the receiving end to perform checksum check. By default, the function is enabled.

Table 40-30 Filling in UDP Packet Checksum

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure to fill in packet checksum in transmitting UDP packets.	<b>ip udp send-checksum</b>	Mandatory By default, the function is enabled.

## 40.2.7 IP Basics Monitoring and Maintaining

Table 40-31 IP Basics Monitoring and Maintaining

Command	Description
<b>clear ip icmpstat</b>	Clears ICMP protocol statistics.
<b>clear ip statistics</b>	Clears IP protocol statistics.
<b>clear ip tcp syncache statistics</b>	Clears TCP protocol syncache statistics.
<b>clear ip tcpstat</b>	Clears TCP protocol statistics.
<b>clear ip udpstat</b>	Clears UDP protocol statistics.
<b>show ip icmpstat</b>	Displaying ICMP protocol statistics.
<b>show ip interface [ <i>interface-name</i>   <b>brief</b> ]</b>	Displaying the interface IP address.
<b>show ip sockets</b>	Displaying the Socket details.
<b>show ip statistics</b>	Displaying IP protocol statistics.
<b>show ip tcpstat</b>	Displaying TCP protocol statistics.
<b>show ip tcp syncache statistics</b>	Displaying TCP syncache statistics.
<b>show ip udpstat</b>	Displaying UDP protocol statistics.
<b>show ip tcp syncache detail</b>	Displaying TCP protocol syncache entry details.

Command	Description
<b>show tcp tcb [ detail ]</b>	Displaying TCP protocol control block details.

# 41 DHCP

---

## 41.1 Overview

It is hard to manage a large network. For example, in a network in which IP addresses are manually allocated, IP address conflicts are common. The only way of solving the problem is to dynamically allocate IP addresses to the hosts. The Dynamic Host Configuration Protocol (DHCP) allocates IP address to requesting hosts from an IP address pool. DHCP also provides other information, such as gateway IP and DNS server address. DHCP reduces the workload of the administrator in recording and tracking manually allocated IP addresses.

DHCP is a protocol that is based on UDP broadcast. The process for a DHCP client to obtain an IP address and other configuration information from a DHCP server contains four phases:

**DISCOVER phase.** When the DHCP client accesses the network for the first time, it sends a DHCP DISCOVER packet with the source address 0.0.0.0 and destination address 255.255.255.255 to the network.

**OFFER phase.** After the DHCP server receives the DHCP DISCOVER broadcast packet sent by the client, it selects an IP address from the corresponding IP address pool according to the policy, and sends the IP address and other parameters to the client in a DHCP OFFER packet.

**REQUEST phase.** If the DHCP client receives response messages from multiple DHCP servers on the network, it selects one DHCP OFFER (usually the one that arrives first). Then it sends a DHCP REQUEST packet to the network, telling all DHCP servers the IP address of which server it will accept.

**ACK phase.** After the DHCP server receives the DHCP REQUEST packet from the DHCP server, it sends a DHCP ACK message containing the provided IP address and other configuration to the DHCP client, telling the DHCP client that the DHCP client can use the provided IP address.

The IP address that the DHCP server allocates to the DHCP client has a lease. After the lease expires, the server will take back the allocated IP address. When the lease term of the IP address of the DHCP client has passed half time, the DHCP client sends a DHCP REQUEST packet to the DHCP server requesting to update its IP address lease. If the DHCP server allows the DHCP client to use its IP address, the DHCP server responds with a DHCP ACK packet, requesting the DHCP client to update the lease. If the DHCP server does not allow the DHCP client to continue to use the IP address, the DHCP server responds with a DHCP NAK packet.

During dynamic IP address acquisition, request packets are sent in broadcast mode; therefore, DHCP is applied only when the DHCP client and server are in the same subnet. If multiple subnets exist in a network and the hosts of the subnets need to obtain configuration information such as IP address through the DHCP server, the hosts of the subnets communicate with the DHCP server through a DHCP relay to obtain IP addresses and other configuration information.

## 41.2 DHCP Function Configuration

Table 41-1 DHCP Function Configuration List

Configuration Task	
Configure a DHCP Address Pool	Creating the DHCP address pool to allow VRF attributes specification.
	Configure an IP address range.
	Configure a DNS server address.
	Configure the default route.
	Configure the lease of an IP address.
	Bind an IP address and a MAC address.
	Configure user-defined options.
	Configure the IP address pool of a specified vender.
Configure other parameters of a DHCP server.	Configure DHCP server.
	Configure the ranges of reserved IP addresses.
	Configure the DHCP ping probe parameters.
	Configure DHCP data logging function.
Configure the functions of a DHCP client.	Configure a DHCP client.
	Configure vendor ID.
	Configure DHCP routing distance.
	Configure DHCP option 60 function.

	Configure the DHCP client not to request the default route option.
Configure the Function of a DHCP Relay	Configure interface DHCP relay.
	Configure functions of Option 82.
	Configure interface DHCP relay packets source address.
	Configure a DHCP server address.

### 41.2.1 Configure a DHCP Address Pool

#### Configuration Condition

None

#### Create a DHCP Address Pool

A DHCP server needs to select and allocate IP addresses and other parameters from a DHCP address pool. Therefore, a DHCP address pool must be created for the DHCP server.

Table 41-2 Creating a DHCP Address Pool

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Create a DHCP address pool and enter the DHCP configuration mode.	<b>ip dhcp pool <i>pool-name</i></b> <b>[ vrf <i>vrf-name</i> ]</b>	Mandatory By default, no DHCP address pool has been created by the system.

#### Note

- Address pools fall into two types: Network and Range. The two types of address pools can be configured respectively through the network and range commands.

### Configure an IP address range.

On a DHCP server, each DHCP address pool must be configured with an IP address range to allocate IP addresses to DHCP clients.

Table 41-41 Configuring an IP Address Range

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the DHCP configuration mode.	<b>ip dhcp pool</b> <i>pool-name</i> [ <b>vrf</b> <i>vrf-name</i> ]	-
Configure an IP address range for an address pool of the Network type.	<b>network</b> <i>ip-address</i> [ <i>network-mask</i>   <i>mask-len</i> ]	Optional By default, an IP address range is not configured for an address pool.
Configure an IP address range for an address pool of the Range type.	<b>range</b> <i>low-ip-address</i> <i>high-ip-address</i> [ <i>network-mask</i>   <i>mask-len</i> ]	Optional By default, an IP address range is not configured for an address pool.

---

### Note

- After an IP address range is configured for an address pool by using the `network` or `range` command, if you run the `network` or `range` command again, the new IP address range configuration overwrites the existing configuration.
  - Change the type of the address pool from `network` to `range` (or vice versa). If the address range of the new configuration and the address range of the old configuration intersect, the command line will prompt the user whether to perform this operation, if yes, all address configurations (static binding, vendor sub-pool) and dynamic leases under the address pool will be deleted; if the actual effective address range of the new configuration covers the actual effective address range of the old configuration, the address pool will keep all the address configurations under the address pool (static binding, vendor sub-pool), and delete the ip range and dynamic lease of the vendor sub-pool configuration.
- 

### Configure a DNS server address.

On a DHCP server, you can configure the DNS server address respectively for each DHCP address pool. When a DHCP server allocates an IP address for a DHCP client, it also sends the DNS server address to the client.

When the DHCP client starts dynamic domain name resolution, it queries the DNS server.

Table 41-3 Configuring a DNS Server Address

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the DHCP configuration mode.	<b>ip dhcp pool</b> <i>pool-name</i> [ <b>vrf</b> <i>vrf-name</i> ]	-
Configure a DNS server address.	<b>dns-server</b> { <i>ip-address</i> &<1-8> / <b>autoconfig</b> }	Mandatory By default, the DNS server address is not configured.

#### Configure the default route.

On a DHCP server, you can specify the address of a gateway corresponding to clients for each DHCP address pool. When the server allocates an IP address to a client, it also sends the gateway address to the client.

When a DHCP client accesses a server or host that is not in the network segment, its data is forwarded through the gateway.

Table 41-4 Configuring the Default Route

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the DHCP configuration mode.	<b>ip dhcp pool</b> <i>pool-name</i> [ <b>vrf</b> <i>vrf-name</i> ]	-
Configure the default route.	<b>default-router</b> <i>ip-address</i> &<1-8>	Mandatory By default, no default route is configured.

#### Configure the lease of an IP address.

The IP address that the DHCP server allocates to the DHCP client has a lease. After the lease expires, the server will take back the allocated IP address. If the DHCP client wants to continue to use the IP address, it must have the IP address lease updated.

On the DHCP server, you can configure an IP address lease for each DHCP address pool.

Table 41-5 Configuring the Lease of an IP Address

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the DHCP configuration mode.	<b>ip dhcp pool <i>pool-name</i></b> <b>[ vrf <i>vrf-name</i> ]</b>	-
Configure the lease of an IP address.	<b>lease <i>days</i> [ <i>hours</i> [ <i>minutes</i> ] ]</b>	Mandatory  By default, the value of <i>days</i> is 1, the value of <i>hours</i> is 6, and the value of <i>minutes</i> is 0.

**Bind an IP address and a MAC address.**

After IP addresses and MAC addresses are bound, when the client with a specified MAC address sends an IP address request to the DHCP server, the DHCP server allocates the IP address that is bound to the IP address to the client. In this way, as long as the MAC address of the client is not changed (e.g., by replacing the network interface card), the client will obtain the same IP address from the server each time.

Table 41-6 Binding IP Addresses and MAC Addresses

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the DHCP configuration mode.	<b>ip dhcp pool <i>pool-name</i></b> <b>[ vrf <i>vrf-name</i> ]</b>	-
Bind an IP address and a MAC address.	<b>bind { <i>ip-address mac-address</i>   <b>automatic</b> }</b>	Mandatory  By default, no IP address and MAC address binding is configured.

**Configure user-defined options.**

For some options, RFC does not give specifications; therefore, you can define these options according to the actual requirement.

Table 41-7 Configuring User-Defined Options

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the DHCP configuration mode.	<b>ip dhcp pool</b> <i>pool-name</i> [ <b>vrf</b> <i>vrf-name</i> ]	-
Configure user-defined options.	<b>option</b> <i>option-code</i> { <b>ascii</b> <i>ascii-string</i>   <b>hex</b> <i>hex-string</i>   <b>ip</b> <i>ip-address</i> &<1-8> }	Mandatory By default, user-defined options are not configured.

### Configure a DHCP Vendor Address Pool

When the client requests an IP address, it may carry the option 60, which specifies the vendor ID. Users can specify different IP address segments for different vendors.

Table 41-8 Configuring a DHCP Vendor Address Pool

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the DHCP configuration mode.	<b>ip dhcp pool</b> <i>pool-name</i> [ <b>vrf</b> <i>vrf-name</i> ]	-
Configure the vendor address pool and enter DHCP vendor address pool configuration mode.	<b>vendor-class-identifier</b> <i>vendor_id</i>	By default, no vendor address pool is configured.
Configure the vendor address pool range.	<b>ip range</b> <i>low-ip-address</i> <i>high-ip-address</i>	No range is configured by default.
Configure the contents of option 43 to be returned by the specified vendor.	<b>option 43</b> { <b>ascii</b> <i>ascii-string</i>   <b>hex</b> <i>hex-string</i>   <b>ip</b> <i>ip-address</i> &<1-8> }	No configured by default.

## 41.2.2 Configure other parameters of a DHCP server.

### Configuration Condition

None

### Configure DHCP server.

After configuring the interface to work in DHCP server mode, when the interface receives DHCP request packets from DHCP clients, the DHCP server allocates IP addresses and other network parameters for the clients.

Table 41-9 Configuring a DHCP Server

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure the functions of the DHCP server.	<b>ip dhcp server</b>	Mandatory By default, no DHCP server function is configured.

### Configure the ranges of reserved IP addresses.

In the DHCP address pool, some IP addresses are reserved for specific devices, and some conflict with the IP addresses of other hosts on the network. These IP addresses cannot be used for dynamic allocation.

Table 41-10 Configuring the Range of Reserved IP Addresses

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the ranges of reserved IP addresses.	<b>ip dhcp excluded-address</b> <i>low-ip-address</i> [ <i>high-ip-address</i> ] [ <b>vrf</b> <i>vrf-name</i> ]	Mandatory By default, the range of reserved IP addresses is not configured.

		The IP addresses in the reserved IP address range will not be allocated.
--	--	--

### Configure DHCP Ping Probe Parameters

To prevent an IP address conflict, before dynamically allocating an IP address to a DHCP client, a DHCP server must detect the IP address. The detection operation is performed with the ping operation. The DHCP server determines whether an IP address conflict exists by checking and whether an ICMP echo response packet is received within the specified time.

Table 41-11 Configuring DHCP Ping Probe Parameters

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the DHCP ping probe parameters.	<b>ip dhcp ping { packets packet-num   timeout milliseconds }</b>	Mandatory By default, the number of ping packets is 1, and the timeout time is 500 ms.

### Configure DHCP data logging function.

When the data log function of a DHCP server is enabled, the address pool allocation on the DHCP server will be recorded to the data log.

Table 41-12 Configuring the DHCP Service Switch

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the DHCP server data logging service switch.	<b>ip dhcp logging security-data</b>	Mandatory By default, the data logging function is not enabled.

### 41.2.3 Configure the functions of a DHCP client.

#### Configuration Condition

None

### Configure a DHCP client.

A DHCP client interface obtains an IP address and other parameters through DHCP.

Table 41-13 Configuring a DHCP Client

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure the DHCP client to obtain an IP address.	<b>ip address dhcp [ request-ip-address ip-address ]</b>	Mandatory By default, the DHCP client is not configured to obtain an IP address.

### Configure DHCP routing distance.

Each protocol in the IP routing table has an administrative distance, or routing distance, that controls routing. Routing distance is used to make routing decisions for the same network segment routes from different protocols, and routes with small routing distance take precedence.

Table 41-14 Configuring DHCP Routing Distance

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure DHCP routing distance.	<b>ip dhcp route-distance</b> <i>distance</i>	Mandatory By default, the DHCP routing distance is 254.

### Configure the Option 60 Function

The content of DHCP option 60 is vendor ID, and the option 60 content can be carried during DHCP client request. The server can set the IP address allocation policy based on this option.

Table 41-15 Configuring DHCP Option 60 Function

Step	Command	Description
------	---------	-------------

Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure the option 60 function.	<b>ip dhcp vendor-class-identifier {disable   content hex-string}</b>	The option 60 content is carried by default.

#### Configure the DHCP client not to request the default route option.

In the process of requesting IP address, the DHCP client, will request the default route by default, users can specify the DHCP client not to request default route so as to configure the route by themselves.

Table 41-16 Configuring the DHCP Client Not to Request the Default Route Option

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the DHCP client not to request the default route option.	<b>ip dhcp router-option disable</b>	Mandatory By default, the DHCP client will request the default route option.

### 41.2.4 Configure the Function of a DHCP Relay

#### Configuration Condition

None

#### Configure a DHCP Relay

If multiple subnets exist in a network and the hosts of the subnets need to obtain configuration information such as IP address through the DHCP server, the hosts of the subnets communicate with the DHCP server through a DHCP relay to obtain IP addresses and other configuration information. If an interface is configured to work in DHCP relay mode, after the interface receives DHCP packets from a DHCP client, it relays the packet to the specified DHCP server. The DHCP server then allocates an IP address.

Table 41-17 Configure a DHCP Relay

Step	Command	Description
------	---------	-------------

Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure the Function of a DHCP Relay	<b>ip dhcp relay</b>	Mandatory  By default, the DHCP relay function is not configured.

### Configure Functions of Option 82

Option 82 is a relay information option, which records the location of a DHCP client. If the DHCP relay is enabled to support Option 82 through configuration, a DHCP relay receives a request packet sent by a DHCP client to a DHCP server and the request packet does not contain the Option 82 option, it adds Option 82 into the request packet and sends the packet to the DHCP server. If the DHCP relay is enabled to support Option 82 through configuration and the request packet carries Option 82, it will proceed to the next step according to the action configured by the **ip dhcp relay information strategy** command, and then forward the packet to the server. If the DHCP relay receives a DHCP response packet which contains Option 82, it deletes Option 82 and forwards the packet to the DHCP client.

Table 41-18 Configuring the Option 82 Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the DHCP relay to support Option 82	<b>ip dhcp relay information option</b>	Mandatory  By default, the DHCP relay is not enabled to support Option 82.
Configure the processing policy when a DHCP relay receives a request packet with Option 82 from a client.	<b>ip dhcp relay information strategy{drop   keep   replace}</b>	Optional  Use the REPLACE action for packets carrying Option 82.
Configure functions of Option 82.	<b>ip dhcp relay information option   remote-id { ascii <i>ascii-string</i>   hex <i>hex-string</i> }   circuit-id { ascii</b>	Mandatory  By default, the Option 82 function is not configured.

	<i>ascii-string</i>   <b>hex hex-string</b> }	
--	---	--

### Configure DHCP Relay Packets Source Address

The source address used by DHCP relay when forwarding DHCP client-originated packets to a DHCP server is, by default, the output interface address of the route to the DHCP server. In some environments, the DHCP server cannot communicate with this address, therefore users are allowed to configure the source address of the packets forwarded by the DHCP relay to the DHCP server and the giaddr field in the packets via the **ip dhcp relay source-address** command. Also users are allowed to configure the DHCP relay source address as the address of the interface that receives DHCP client packets via the **ip dhcp relay source-address relay-address** command.

Table 41-19 Configuring DHCP Relay Packets Source Address

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure DHCP Relay Packets Source Address	<b>ip dhcp relay source-address relay-address</b>	Mandatory By default, the DHCP relay packets source address is the output interface address of the route to the DHCP server.
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure DHCP Relay Packets Source Address	<b>ip dhcp relay source-address</b> <i>ip-address</i>	Mandatory By default, the DHCP relay packets source address is the output interface address of the route to the DHCP server.

### Note

- The source address of the **ip dhcp relay source-address** *ip-address* configuration must be the interface address of this device, and the interface address must belong to the same vrf

---

as the relay interface, otherwise the relay packets will fail to be sent.

- If the **ip dhcp relay source-address** *ip-address* command is configured in interface mode and the **ip dhcp relay source-address relay-address** command is configured in global mode, the former has a higher priority than the latter, and the DHCP relay will fill the configured *ip-address* with the source address of DHCP relay packets sent to the DHCP server.
- 

### Configure a DHCP server address.

After the interface receives DHCP packets from a DHCP client, it relays the packet to the specified DHCP server. The DHCP server then allocates an IP address.

Table 41-20 Configuring a DHCP Server Address

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure a DHCP server address.	<b>ip dhcp relay server - address</b> <i>ip-address</i>	Mandatory By default, no DHCP server address is configured.

## 41.2.5 DHCP Monitoring and Maintaining

Table 41-21 DHCP Monitoring and Maintaining

Command	Description
<b>clear ip dhcp pool</b> <i>pool-name</i> { <b>lease</b>   <b>conflict</b> [ <i>ip-address</i> ] }	Clears dynamic lease information from the address pool or address information with conflicting addresses.
<b>clear ip dhcp server interface</b> [ <i>interface-name</i> ] <b>statistics</b>	Clears the key statistics when the DHCP server interacts with clients or relays for packets.
<b>clear ip dhcp relay statistics</b>	Clears the statistics on the DHCP relay device.

<pre><b>show ip dhcp server interface</b> <i>interface-name</i> [<b>statistics</b>]</pre>	<p>Displaying the address pool information associated with the specified interface or displaying the key statistics when the DHCP server engages in packet interactions with clients or relays under the specified interface.</p>
<pre><b>show ip dhcp pool</b> <i>pool-name</i> { <b>summary</b>   <b>ping_list</b>   <b>offer_list</b>   <b>excluded_list</b>   <b>conflict_list</b>   <b>lease</b>   <b>binding</b> }</pre>	<p>Displaying the summary information of the specified address pool or the information of the address that is doing ping check or the address that has sent the OFFER packet and is waiting for the DHCP client to respond to the REQUEST packet or the information of the excluded address in the address pool or the information of the address that has address conflict in the address pool or the information of dynamic lease in the address pool or the information of static binding in the address pool.</p>
<pre><b>show ip dhcp pool</b> <i>pool-name</i> <b>specific</b> { <b>ip-address</b> <i>ip-address</i>   <b>mac-address</b> <i>mac-address</i> }</pre>	<p>Displaying information about the specified IP address or mac address in the address pool.</p>
<pre><b>show ip dhcp relay</b> [<b>interface</b> <i>interface-name</i> ]</pre>	<p>Displaying the packet statistics on the DHCP relay device.</p>

## 41.3 Typical Configuration Example of DHCP

### 41.3.1 Configure a DHCP Server to Statically Allocate IP Addresses

#### Network Requirements

- Device2 acts as a DHCP server to allocate IP addresses, gateway IP addresses, and DNS server IP addresses in a static manner.
- The DHCP server allocates an IP address to PC in MAC binding mode.

#### Network Topology

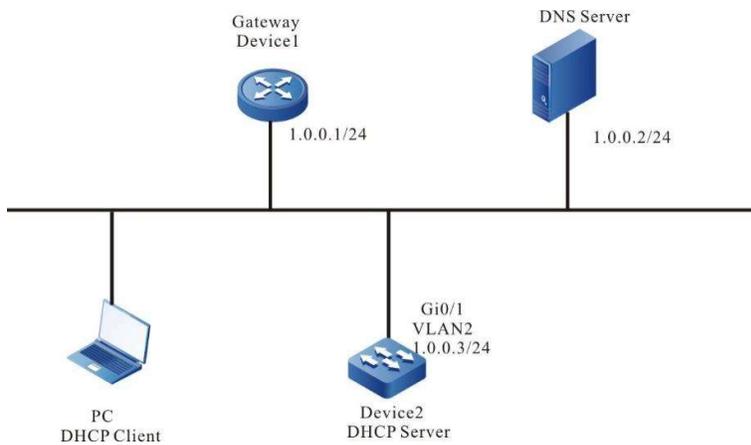


Figure 41-1 Network Topology for Configuring DHCP Server to Statically Allocate IP Addresses

### Configuration Steps

Step 1: Configure Device2 interface IP addresses and enable it to work in DHCP server mode.

```
Device2#configure terminal
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ip address 1.0.0.3 255.255.255.0
Device2(config-if-vlan2)#ip dhcp server
Device2(config-if-vlan2)#exit
```

Step 2: Configure statically bound address pools and parameters.

#Configure the address pool mac-binding, and allocate an IP address to PC in static MAC binding mode.

```
Device2(config)#ip dhcp pool mac-binding
Device2(dhcp-config)#range 1.0.0.4 1.0.0.254 255.255.255.0
Device2(dhcp-config)#bind 1.0.0.11 00e0.00e1.013d
Device2(dhcp-config)#default-router 1.0.0.1
Device2(dhcp-config)#dns-server 1.0.0.2
Device2(dhcp-config)#exit
```

Step 3: Check the result.

#On Device2, use the show ip dhcp server interface vlan2 command to check the address pool associated with the interface.

```
Device2(config)#exit
Device2#show ip dhcp server interface vlan2
DHCP server status information:
DHCP server is enabled on interface: vlan2
Vrf: global
DHCP server pool information:
Available directly-connected pool:
Interface IP    Pool name    Pool Range    Pool utilization
-----
1.0.0.3/24    mac-binding  1.0.0.4 – 1.0.0.254  0.00%
```

#On Device2, use the show show ip dhcp pool mac-binding binding command to check the IP addresses allocated

to the PC.

```
Device2#show ip dhcp pool mac-binding binding
IP Address    MAC Address    Vendor Id    Type    Time Left(s)
-----
```

```
1.0.0.11 00e0.00c1.013d Global Binding NA
```

#On Device2, use the show show ip dhcp pool mac-binding lease command to check the addresses allocated to the PC.

```
Device#show ip dhcp pool danymic-pool2 lease
IP Address      MAC Address      Vendor Id      Type   Time Left(s)
-----
1.0.0.11       00e0.00c1.013d  Global        Lease  107980
```

On the PC, check whether the obtained IP addresses, gateway IP addresses, and DNS server IP addresses are correct.

### 41.3.2 Configure a DHCP Server to Dynamically Allocate IP Addresses

#### Network Requirements

- Two interface VLANs of Device, VLAN2 and VLAN3, are respectively configured with IP addresses in the 1.0.0.3/24 and 2.0.0.3/24 network segments.
- The DHCP server Device dynamically allocates IP addresses in the 1.0.0.0/24 and 2.0.0.0.0/24 network segments to the two clients in the directly-connected physical network.
- The addresses in network segment 1.0.0.0/24 have a one-day lease, the gateway address is 1.0.0.3, the DNS server address is 2.0.0.4. The addresses in network segment 2.0.0.0/24 have a three-day lease, the gateway address is 2.0.0.3, and the DNS server address is 2.0.0.4.
- The first 10 IP addresses in network segments 1.0.0.0/24 and 2.0.0.0/24 are reserved and cannot be allocated.

#### Network Topology

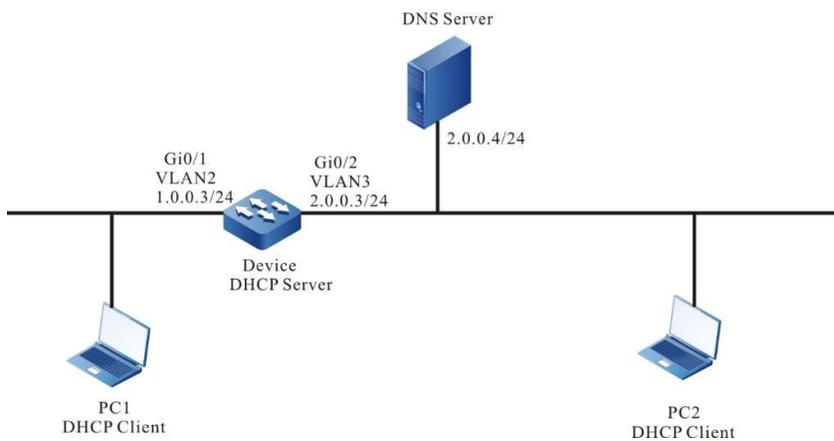


Figure 41-2 Network Topology for Configuring DHCP to Dynamically Allocate IP Addresses

#### Configuration Steps

Step 1: Configure Device interface IP addresses and enable it to work in DHCP server mode.

```
Device(config)#interface vlan2
Device(config-if- vlan2)#ip address 1.0.0.3 255.255.255.0
Device(config-if- vlan2)#ip dhcp server
Device(config-if- vlan2)#exit
Device(config)#interface vlan3
Device(config-if- vlan3)#ip address 2.0.0.3 255.255.255.0
Device(config-if- vlan3)#ip dhcp server
Device(config-if- vlan3)#exit
```

Step 2: On the DHCP server Device, configure two dynamic address pools and their parameters.

#Configure the first 10 IP addresses in the two address pools to be reserved.

```
Device(config)#ip dhcp excluded-address 1.0.0.1 1.0.0.10
Device(config)#ip dhcp excluded-address 2.0.0.1 2.0.0.10
```

#Configure address pool dynamic-pool1 and its parameters (including address range, gateway, DNS, address lease, and local domain name).

```
Device(config)#ip dhcp pool dynamic-pool1
Device(dhcp-config)#network 1.0.0.0 255.255.255.0
Device(dhcp-config)#default-router 1.0.0.3
Device(dhcp-config)#dns-server 2.0.0.4
Device(dhcp-config)#lease 1 0 0
Device(dhcp-config)#exit
```

#Configure address pool dynamic-pool2 and its parameters (including address range, gateway, DNS address, address lease, Wins server address, and local domain name).

```
Device(config)#ip dhcp pool dynamic-pool2
Device(dhcp-config)#network 2.0.0.0 255.255.255.0
Device(dhcp-config)#default-router 2.0.0.3
Device(dhcp-config)#dns-server 2.0.0.4
Device(dhcp-config)#lease 3 0 0
Device(dhcp-config)#exit
```

Step 3: Check the result.

#View information about the server-associated address pool on Device.

```
Device(config)#exit
Device#show ip dhcp server interface vlan2
DHCP server status information:
DHCP server is enabled on interface: vlan2
Vrf : global
DHCP server pool information:
Available directly-connected pool:
Interface IP   Pool name   Pool Range   Pool utilization
-----
1.0.0.3/24    dynamic-pool1  1.0.0.0 – 1.0.0.255  0.00%
Device#show ip dhcp server interface vlan3
DHCP server status information:
DHCP server is enabled on interface: vlan3
Vrf : global
DHCP server pool information:
Available directly-connected pool:
Interface IP   Pool name   Pool Range   Pool utilization
-----
1.0.0.3/24    dynamic-pool2  2.0.0.0 – 2.0.0.255  0.00%
```

#On Device, query the IP addresses allocated to clients.

```
Device#show ip dhcp pool danymic-pool1 lease
IP Address   MAC Address   Vendor Id   Type   Time Left(s)
-----
1.0.0.11     0001.7a6a.0268  Global    Lease  86390
Device#show ip dhcp pool danymic-pool2 lease
```

IP Address	MAC Address	Vendor Id	Type	Time Left(s)
2.0.0.11	0001.7a6a.0269	Global	Lease	259194

#On Device, query the IP address pool allocation statistics.

```
Device#show ip dhcp pool dynamic-pool1 summary
```

```
Pool: dynamic-pool1
Pool Configuration : 1.0.0.0 255.255.255.0
Pool Range       : 1.0.0.0 1.0.0.255
Pool Utilization : 0.39%
VRF              : global
DNS Server       : 2.0.0.4
Default Router   : 1.0.0.3
Lease Time       : 1 Days 0 Hours 0 Minutes
Free Addresses   : 243
Static Bind      : 0
Lease Count      : 1
PingList        : 0
OfferList       : 0
ConflictList    : 0
ExcludeList     : 12
```

```
Device#show ip dhcp pool dynamic-pool2 summary
```

```
Pool: dynamic-pool2
Pool Configuration : 2.0.0.0 255.255.255.0
Pool Range       : 2.0.0.0 2.0.0.255
Pool Utilization : 0.39%
VRF              : global
DNS Server       : 2.0.0.4
Default Router   : 2.0.0.3
Lease Time       : 3 Days 0 Hours 0 Minutes
Free Addresses   : 243
Static Bind      : 0
Lease Count      : 1
PingList        : 0
OfferList       : 0
ConflictList    : 0
ExcludeList     : 12
```

On the DHCP clients, query whether the IP addresses have been obtained properly.

---

## Caution

- The IP addresses in the address pool must be within the network segment range of the interface that provides the service.
- 

### 41.3.3 Configure a DHCP Relay

#### Network Requirements

- Device1 is the DHCP server and Device2 interface is enabled for DHCP relay function.
- The DHCP server serves clients in the 1.0.0.0/24 network segment, and the first 10 IP addresses are reserved.
- DHCP client obtains IP address through DHCP relay.

#### Network Topology

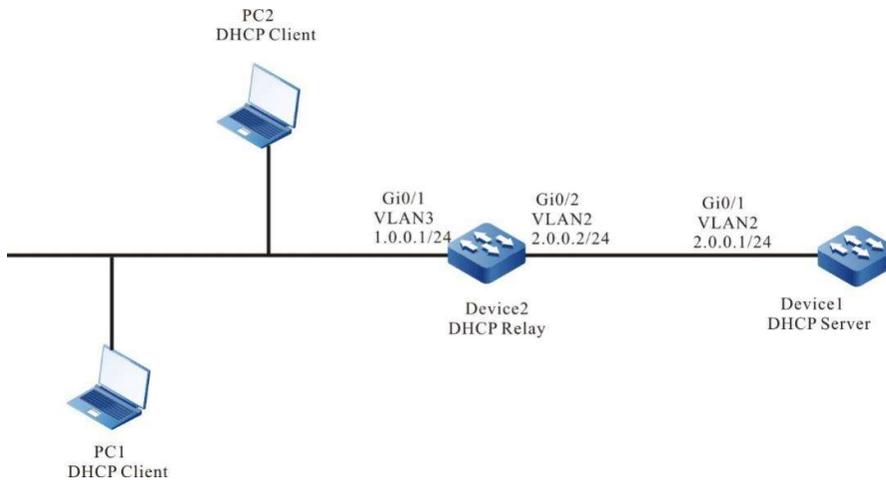


Figure 41-3 Network Topology for Configuring DHCP Relay

### Configuration Steps

Step 1: Configure VLANs, and add ports to the required VLANs. Configure IP addresses for the ports. (Omitted)

Step 2: Configure the IP address pool and the reserved IP addresses of Device1, and enable it to work in the DHCP server mode.

#Configure the DHCP server.

```
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ip dhcp server
Device1(config-if-vlan2)#exit
```

#Configure IP addresses which are from 1.0.0.1 to 1.0.0.10 not to be allocated.

```
Device1#configure terminal
Device1(config)#ip dhcp excluded-address 1.0.0.1 1.0.0.10
```

#Configure IP address pool dynamic-pool for Device1.

```
Device1(config)#ip dhcp pool dynamic-pool
Device1(dhcp-config)#network 1.0.0.0 255.255.255.0
Device1(dhcp-config)#default-router 1.0.0.1
Device1(dhcp-config)#lease 1 0 0
Device1(dhcp-config)#exit
```

#Configure a static route to network segment 1.0.0.0/24.

```
Device1(config)#ip route 1.0.0.0 255.255.255.0 2.0.0.2
```

Step 3: On the vlan3 interface of Device2, configure the IP address of the DHCP server to be 2.0.0.1, and enable the interface to work in relay mode.

```
Device2(config)#interface vlan3
Device2(config-if-vlan3)#ip dhcp relay
Device2(config-if-vlan3)#ip dhcp relay server-address 2.0.0.1
Device2(config-if-vlan3)#exit
```

Step 4: Check the result.

#On Device1, check the IP addresses that have been allocated.

```

Device1#show ip dhcp pool dynamic-pool lease
IP Address      MAC Address      Vendor Id      Type      Time Left(s)
-----
1.0.0.11       0001.7a6a.0268  Global        Lease     86387

```

Use the `show ip dhcp pool dynamic-pool lease` command to query the IP addresses that have been allocated to clients.

The result shows that a client has obtained the IP address 1.0.0.11.

### 41.3.4 Configure the DHCP Relay to Support Option 82.

#### Network Requirements

- On the DHCP relay device, Option 82 is enabled.
- Specify the content of Option 82 sub-option Remote ID as 0102030405.
- The DHCP relay Device2 adds Option 82 in a request packet and forwards the request to DHCP server. The DHCP server then allocates IP addresses in the 1.0.0.0/24 network segment to the client.

#### Network Topology

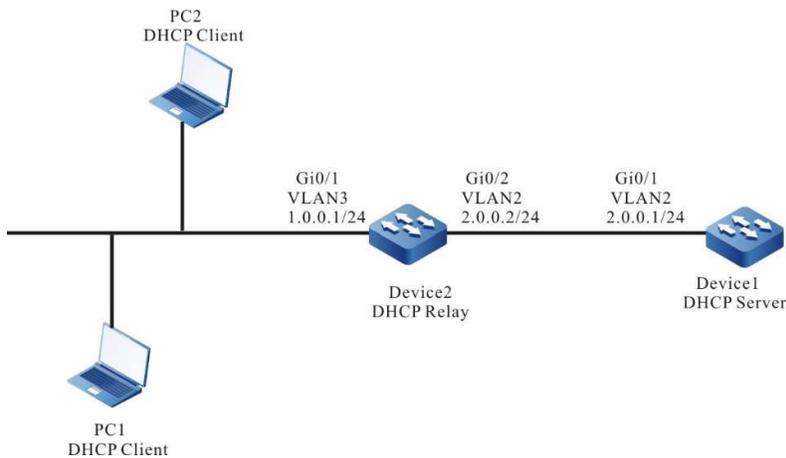


Figure 41-4 Network Topology for Configuring DHCP Relay to Support Option 82

#### Configuration Steps

Step 1: Configure VLANs, and add ports to the required VLANs. Configure IP addresses for the ports. (Omitted)

Step 2: Configure the DHCP server.

```

Device1# configure terminal
Device1(config)#interface vlan2

```

```
Device1(config-if-vlan2)#ip dhcp server
Device1(config-if-vlan2)#exit
Device1(config)#ip dhcp pool dynamic-pool
Device1(dhcp-config)#network 1.0.0.0 255.255.255.0
Device1(dhcp-config)#default-router 1.0.0.1
Device1(dhcp-config)#exit
```

#Configure a static route to network segment 1.0.0.0/24.

```
Device1(config)#ip route 1.0.0.0 255.255.255.0 2.0.0.2
```

Step 3: Configure the DHCP relay Device2 and Option 82 parameters.

#Configure the IP address of the DHCP relay server to 2.0.0.1.

```
Device2(config)#interface vlan3
Device2(config-if-vlan3)#ip dhcp relay
Device2(config-if-vlan3)#ip dhcp relay server-address 2.0.0.1
```

#Enable Option 82, and configure the sub-option Remote-ID to 0102030405.

```
Device2(config)#ip dhcp relay information option
Device2(config)#ip dhcp relay information remote-id hex 0102030405
```

Step 4: Check the result.

#On Device1, query the IP addresses allocated to clients.

```
Device1#show ip dhcp pool danymic-pool1 lease
IP Address      MAC Address      Vendor Id      Type      Time Left(s)
-----
1.0.0.2         0001.7a6a.0268   Global         Lease     107992
```

On the DHCP client, query the IP address that the network adapter has obtained from network segment 1.0.0.0/24.

Packet capture on the DHCP server end can verify that the padding value of the remote-id of option 82 in the discover packets received by the server is

0102030405.

---

## Note

- After Option 82 is enabled, its sub-option Circuit ID is filled with the receiving interface index and the system ID of the relay device.
-

# 42 DNS

---

## 42.1 Overview

Domain Name System (DNS) is a distributed database that maps domain names and IP addresses. It provides conversion between domain names and IP addresses. With the use of DNS, when users access the Internet, they can use easy-to-memory and meaningful domain names. Then the domain name server in the network resolves the domain names into correct IP addresses. DNS is categorized into static DNS and dynamic DNS.

Static domain name resolution is conducted through a static DNS table. In the static DNS table, domain names and IP addresses are mapped, and some frequently used domain names are added. When a client requests for the IP address of a domain name, the DNS server first searches static DNS table for the corresponding IP address. This improves the efficiency of domain name resolution.

Dynamic domain name resolution is implemented by querying the DNS. A DNS client sends a domain name resolution request to a DNS server. After the DNS server receives the domain name resolution request, it first determines whether the requested domain name is located in its authorized management sub-domain. If yes, it searches the database for the required IP address and then sends the query result to the client. If the domain name is not in the authorized management sub-domain, the DNS server starts a recursive resolution with other DNS server, and then it sends the resolution result to the client. Alternatively, it specifies the address of the next DNS server in the response packet to the DNS client. Then, the client sends another domain name resolution request to the domain name server. This is so called iterative resolution mode.

## 42.2 DNS Function Configuration

Table 42-1 DNS Function Configuration List

Configuration Task	
Configure DNS cache specifications.	Configure the maximum number of static cache.
	Configure the maximum number of dynamic cache.

Configuration Task	
Configure the DNS client function.	Configure static domain name resolution.
	Configure dynamic domain name resolution.
Configure DNS probe function.	Configure domain name list.
	Detect domain name resolution.

### 42.2.1 Configure DNS cache specifications.

#### Configuration Condition

None

#### Configure DNS specifications

Modify the maximum number of entries supported by DNS specification, if the current specification is M, the current number is n; the configured specification is N; the two scenarios are as follows

1. For static specification, if  $N > M$  or  $n < N < M$ ; the configuration takes effect immediately; if  $N < n$ ; the configuration is prompted to have failed.
2. For dynamic specification, if  $N > M$  or  $n < N < M$ ; the configuration takes effect immediately; if  $N < n$ ; the configuration takes effect, wait for the aging of dynamic DNS.

Table 42-2 List for Configuring Privileged Mode Authentication Methods

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the maximum number of configurable specifications supported by static dns.	<b>dns static max-count</b> <i>number</i>	Optional By default, the maximum number supported by static cache is 64.
Configure the maximum number supported by dynamic dns for configuration.	<b>dns dynamic max-count</b> <i>number</i>	Optional By default, the maximum number supported by dynamic cache is 10k.

## 42.2.2 Configure the DNS client function.

### Configuration Condition

None

### Configure static domain name resolution.

Configuring static domain name resolution is to configure a domain name to map an IPv4 address and an IPv6 address.

Table 42-3 Configuring Static Domain Name Resolution

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure a domain name and its corresponding IPv4 address.	<b>ip host [ vrf vrf-name ] domain-name ip-address</b>	Mandatory  By default, no domain name and its corresponding IPv4 address are configured.
Configure a domain name and its corresponding IPv6 address.	<b>ipv6 host [ vrf vrf-name ] domain-name ipv6-address</b>	Mandatory  By default, no domain name and its corresponding IPv6 address are configured.

### Configure dynamic domain name resolution.

In configuring dynamic domain name resolution, you need to configure the IP address of a domain name server. Then, domain resolution requests can be sent to the proper domain server for resolution.

Users can pre-configure a domain suffix. Then, when the users use a domain name, they can input only part fields of the domain name, and the system automatically adds pre-configured domain suffix for resolution.

Table 42-4 Configuring Dynamic Domain Name Resolution

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Configure a domain suffix.	<b>ip domain-name</b> [ <b>vrf vrf-name</b> ] <i>domain-name</i>	Mandatory By default, no domain suffix is configured.
Configure a DNS server address.	<b>ip name-server</b> [ <b>vrf vrf-name</b> ] <i>ip-address</i>	Mandatory By default, the DNS server address is not configured.

### 42.2.3 Configure DNS probe function.

#### Configuration Condition

None

#### Configure domain name list.

By configuring the domain name list, you can add some commonly used domain names to the domain name list and save them, and when you need to use them, you can directly specify the name of the domain name list.

Table 42-5 Configuring the Domain Name List

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Create a domain list and enter domain list configuration mode.	<b>dns domain-list</b> <i>list-name</i>	Mandatory By default, no domain name list is configured.
Configure domain name.	<b>domain</b> <i>domain-name</i>	Mandatory By default, no domain name is configured from the domain name list.

#### Detect domain name resolution.

By detecting domain name resolution, you can check whether the DNS server can correctly resolve the specified domain name.

Table 42-6 Detecting Domain Name Resolution

Step	Command	Description
Detect domain name resolution.	<b>dns query</b> [ <b>vrf</b> <i>vrf-name</i> ] <i>ip-address</i> [ <b>name</b> <i>domain-name</i>   <b>name-list</b> <i>list-name</i> ] [ <b>timeout</b> <i>time</i> ]	Mandatory  By default, domain name resolution is not detected.

## 42.2.4 DNS Monitoring and Maintaining

Table 42-7 DNS Monitoring And Maintaining

Command	Description
<b>debug dns</b> { <b>all</b>   <b>config</b>   <b>event</b>   <b>mpos</b>   <b>packet</b>   <b>timer</b> }	Turn on the DNS debugging information switch.
<b>show dns domain-list</b> [ <i>list-name</i> ]	Displaying domain name list.
<b>show hosts</b>	Displaying domain name resolution table entries.
<b>show name-server</b> [ <i>vrf vrf-name</i> ]	Displaying DNS server information.

## 42.3 Typical Configuration Example of DNS

### 42.3.1 Configure static domain name resolution.

#### Network Requirements

- Device and PC are interconnected, and the route is reachable.
- The host name of PC is host.xxyyz.com, and the IP address is 1.0.0.2/24.
- On Device, access the host host.xxyyz.com through static domain name resolution.

#### Network Topology

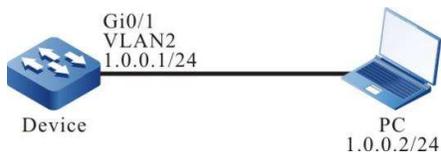


Figure 42-1 Network Topology for Configuring Static Domain Name Resolution

### Configuration Steps

Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configure IP addresses for the ports. (Omitted)

Step 3: Configure a static domain name.

#On Device, configure the host name host.xxyzz.com to correspond to IP address 1.0.0.2.

```
Device#configure terminal
Device(config)#ip host host.xxyzz.com 1.0.0.2
Device(config)#exit
```

Step 4: Check the result.

#On Device, ping host host.xxyzz.com. Device obtains the IP address 1.0.0.2 that corresponds to the host name through local domain name resolution.

```
Device#ping host.xxyzz.com

Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 1.0.0.2 , timeout is 2 seconds:
!!!!
Success rate is 100% (5/5). Round-trip min/avg/max = 0/6/16 ms.
```

---

#### 说明:

- In pinging a host name, the IPv6 address corresponding to the host name is first resolved, and then the IPv4 address.
- 

## 42.3.2 Configure dynamic domain name resolution.

### Network Requirements

- The IP address of the DNS server is 1.0.0.3/24, the IP address of Device is 1.0.0.1/24, and the IP address of PC is 1.0.0.2/24.
- The DNS server, Device, and PC are interconnected through a LAN, and the route is

reachable. On the DNS server, the DNS record of host.xxyzz.com and 1.0.0.2 exists.

- Device access PC through dynamic resolution of host.xxyzz.com through the DNS server.

### Network Topology

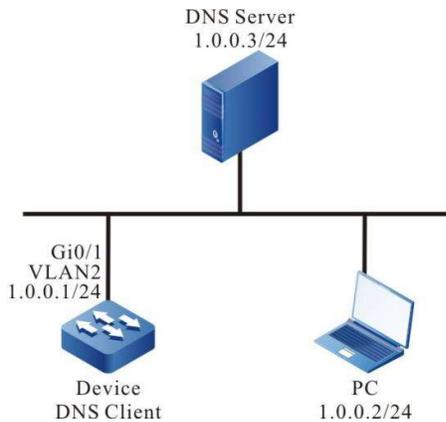


Figure 42-2 Network Topology for Configuring Dynamic Domain Name Resolution

### Configuration Steps

Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configure IP addresses for the ports. (Omitted)

Step 3: Configure the DNS server. (Omitted)

Step 4: Configure the DNS client.

#Specify a DNS server for the client, and the IP address is 1.0.0.3.

```
Device#configure terminal
Device(config)#ip name-server 1.0.0.3
Device(config)#exit
```

Step 5: Check the result.

#On Device, ping host host.xxyzz.com. Device obtains the IP address 1.0.0.2 that corresponds to the host name through the DNS server.

```
Device#ping host.xxyzz.com

Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 1.0.0.2 , timeout is 2 seconds:
!!!!
Success rate is 100% (5/5). Round-trip min/avg/max = 0/6/16 ms.
```

# 43 IPv6 Basics

## 43.1 Overview

IPv6 (Internet Protocol Version 6) is the second generation standard protocol for network layer protocols, also known as IPng (IP Next Generation), which is a set of specifications designed by the IETF (Internet Engineering Task Force) and is an upgraded version of IPv4.

### L3 Interface ND Proxy

The L3 interface ND proxy is used to enable communication between different network segments connected via two interfaces. Normally, the device will not respond to NS requests whose target is not the corresponding network segment of the packet-receiving interface, so different network segments cannot communicate directly. When the ND proxy function is enabled for a L3 interface, the device is also able to answer NA if it receives NS requests from that interface that belongs to another interface network segment. This allows hosts belonging to different network segments to establish neighbor table entries and communicate normally with each other. The typical application scenario is small and large network segment networking.

## 43.2 IPv6 Basic Function Configuration

Table 43-1 IPv6 Basic Function Configuration List

Configuration Task	
Configure IPv6 address.	Configure IPv6 addresses for the ports.
Configure the basic functions of IPv6.	Enable IPv6 unicast forwarding function.
	Enable interface IPv6 function.
	Configure IPv6 packet hop limit value.
	Configure IPv6 MTU for the interface.
Configure IPv6 Neighbor Discovery Protocol.	Configure IPv6 Static Neighbors.
	Configure the aging time of IPv6 neighbor table entries in STALE state.
	Configure the retransmission interval of NS packets.

Configuration Task	
	Configure the attempts to send an NS packet during the IPv6 duplicate address detection.
	Configure the relevant parameters of RA packets.
	Enables the interface to send redirected packets.
Configure to enable the ND fast response function.	Configure to enable the ND fast response function.
Configure L3 interface ND proxy function.	Configure to enable ND proxy function for L3 interface.
Configure ICMPv6 functions.	Configure ICMPv6 error packets transmitting rate.
	Enable transmission of ICMPv6 destination unreachable packets.
Configure TCP anti-attack function for IPv6.	Enable TCP syncache function.
	Enable TCP syncookies function.

### 43.2.1 Configure IPv6 addresses for the ports.

The most significant difference between IPv6 and IPv4 is: the length of IP addresses increases from 32 bits to 128 bits. IPv6 addresses are represented as a series of 16-bit hexadecimal numbers separated by a colon (:). Each IPv6 address is divided into 8 groups, with each group of 16 bits represented by 4 hexadecimal numbers, separated by colons between the groups, e.g. 2000:0000:240F:0000:0000:0CB0:123A:15AB.

To simplify the representation of IPv6 addresses, the "0" in an IPv6 address can be handled in the following way:

The leading "0" in each group can be omitted, i.e. the above address can be expressed as 2000:0:240F:0:0:CB0:123A:15AB.

If the address contains two or more consecutive groups that are all zeros, a double colon "::" can be used instead, i.e. the above address can be expressed as 2000:0:240F::CB0:123A:15AB.

The double colon "::" can only be used once in an IPv6 address, otherwise when the device transforms "::" to 0 to recover the 128-bit address, it will not be able to determine the number of zeros "::" represented.

An IPv6 address consists of two parts: the address prefix and the interface identifier. The address prefix is equivalent to the network number field in an IPv4 address and the interface identifier is equivalent to the host number field in an IPv4 address.

The IPv6 address prefix is expressed as: IPv6 address/prefix length. The IPv6 address is either of the forms listed earlier, and the prefix length is a decimal number indicating the number of bits precede the IPv6 address as the address prefix.

There are three types of IPv6 addresses: unicast addresses, multicast addresses, and anycast addresses.

**Unicast address:** Used to uniquely identify an interface, similar to the unicast address of IPv4. Data packets sent to a unicast address will be delivered to the interface identified by this address.

**Multicast address:** Used to identify a group of interfaces, similar to the multicast address of IPv4. Data packets sent to a multicast address are delivered to all interfaces identified by this address.

**Anycast address:** Used to identify a group of interfaces. A packet destined for an anycast address will only be delivered to one interface in that group. According to the routing protocol, the interface that receives the packet is the interface closest to the source.

The IPv6 address type is specified by the first few bits of the address, called the format prefix. The correspondence between the main address types and the format prefix is shown in Table 5-2.

Table 43-2 Correspondence between IPv6 address types and format prefixes

Address Type		Format prefix (binary)	Prefix identifier
Unicast address	Unallocated address	00...0 (128 bits)	::/128
	Loopback address	00...1 (128 bits)	::1/128
	Link-local address	1111111010	FE80::/10
	Site-local address	1111111011	FEC0::/10
	Global unicast address	Other forms	-
Multicast address		11111111	FF00::/8
Anycast address		Allocate from the unicast address space, using the unicast address format.	

There can be various types of IPv6 unicast addresses, including global unicast addresses, link-local addresses, and site-local addresses.

Global unicast addresses are equivalent to IPv4 public network addresses and are provided to network service providers. This type of address allows aggregation of routing prefixes, thus limiting the number of global routing table entries.

The link-local address is used for communication between nodes on the link-local in the Neighbor Discovery Protocol and Stateless Auto-configuration. Data packets that use link-local addresses as source or destination addresses are not forwarded to other links.

The site-local address is similar to the private address in IPv4. Data packets that use the site-local address as the source or destination address are not forwarded to other sites outside this site.

Loopback address: The unicast address 0:0:0:0:0:0:1 (simplified as ::1) is called a loopback address and cannot be allocated to any physical interface. It serves the same purpose as the loopback address in IPv4, which is used by the node to send IPv6 packets to itself.

Unallocated address: The address "::" is called an unallocated address and cannot be allocated to any node. Until a node obtains a valid IPv6 address, it can fill in the source address field of a sent IPv6 packet, but it cannot be used as the destination address in an IPv6 packet.

The special-purpose multicast addresses reserved for IPv6 are shown in Table 5-3.

Table 43-3 List of IPv6 Special Purpose Multicast Addresses

Address	Use
FF01::1	Indicates the multicast address of all nodes in the local range of the node.
FF02::1	Indicates the multicast address of all nodes in the local range of the link.
FF01::2	Indicates the multicast address of all routers in the local range of the node.
FF02::2	Indicates the multicast address of all routers in the local range of the link.
FF05::2	Indicates the multicast address of all routers in the local range of the site.

**Configuration Condition**

None

**Configure IPv6 addresses for the ports.**

Table 43-4 Configuring Interface IPv6 Addresses

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure IPv6 addresses for the ports.	<b>ipv6 address</b> { <i>linklocal-address link-local</i>   <i>prefix-address [ anycast   eui-64 ]</i>   <b>autoconfig</b> }	Mandatory By default, the interface is not configured with IPv6 address.

 **Note**

- The interface can be configured with multiple IPv6 addresses.

- After the interface is configured with an IPv6 address, the IPv6 function is automatically enabled.

### 43.2.2 Configure the basic functions of IPv6.

#### Configuration Condition

None

#### Enable IPv6 unicast forwarding function.

By default, the IPv6 unicast forwarding function is enabled. In some specific cases, users can turn off the IPv6 unicast forwarding feature, and when the feature is turned off, no IPv6 packets are forwarded.

Table 43-5 Enabling IPv6 Unicast Forwarding

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable IPv6 unicast forwarding function.	<b>ipv6 unicast-routing</b>	Mandatory By default, the IPv6 unicast forwarding function is enabled.

#### Enable interface IPv6 function.

Before making IPv6-related configurations on the interface, you must enable the IPv6 function first, otherwise it may cause some configurations fail to take effect.

Table 43-6 Enabling Interface IPv6 Functions

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface <i>interface-name</i></b>	-

Enable interface IPv6 function.	<b>ipv6 enable</b>	Mandatory By default, the interface IPv6 function is disabled.
---------------------------------	--------------------	---

### Configure IPv6 packet hop limit value.

The IPv6 packet header contains the Hop Limit field, which serves the same purpose as the TTL field in the IPv4 header, indicating the number of times the packet can be forwarded by the router in the network.

The value of the hop limit in the header of IPv6 packet generated by the device can be configured by a command.

Table 43-7 Configuring IPv6 Packet Hop Limit Value

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure IPv6 packet hop limit value.	<b>ipv6 hop-limit <i>value</i></b>	Mandatory By default, the number of hops a device can send IPv6 packets is limited to 64.

### Configure IPv6 MTU for the interface.

Table 8-9 Configuring IPv6 MTU for an Interface

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface <i>interface-name</i></b>	-
Configure IPv6 MTU for the interface.	<b>ipv6 mtu <i>value</i></b>	Mandatory By default, the IPv6 MTU of an interface is not configured.

---

### 43.2.3 Configure IPv6 Neighbor Discovery Protocol.

The IPv6 Neighbor Discovery (ND: Neighbor Discovery) protocol includes the following functions: address resolution, neighbor un-reachability detection, duplicate address detection, router discovery/prefix discovery, address auto-configuration, and redirection.

The types of ICMPv6 packet used by the ND protocol and their functions are shown in Table 5-9 below.

Table 43-10 ICMPv6 Packet Types Used by ND Protocol and Their Functions

Types of ICMPv6 Packets	Type No.	effect
Router Solicitation packet (RS)	133	After the node starts, it sends a request to the router via RS packet to request the prefix and other configuration information for the automatic configuration of the node.
Router Advertisement packet (RA)	134	Responding to a RS packet Under the condition that RA packets are not suppressed, the router periodically sends RA packets, which include prefix information options and flag bits information.
Neighbor Solicitation packet (NS)	135	Obtain the link layer address of a neighbor. Verify if the neighbor is reachable. Perform duplicate address detection.
Neighbor Advertisement packet (NA)	136	Respond to NS packets. The node actively sends out NA packets when the link layer changes to notify neighbor nodes of the changes in this node.
Redirect packets (Redirect).	137	When certain conditions are met, the default gateway redirects the host to reselect the correct next-hop address for subsequent packets by sending a redirect packet to the source host.

#### Address resolution

Obtain the link layer address of neighboring nodes on the same link, which is achieved by NS packets and NA packets.

### **Neighbor Un-reachability Detection**

After obtaining the link layer address of the neighbor node, the NS packets and NA packets can be used to verify the reachability of the neighbor node.

- 1) The node sends an NS packet, where the destination address is the IPv6 address of a neighbor node.
- 2) If an acknowledgment packet is received from a neighbor node, the neighbor is considered reachable; otherwise, the neighbor is considered unreachable.

### **Duplicate Address Detection**

When a node acquires an IPv6 address, it needs to use the duplicate address detection function to determine whether the address is already in use by another node.

### **Router Discovery/Prefix Discovery and Address Auto-Configuration**

Router discovery/prefix discovery means that the node obtains the prefixes of neighbor routers and their networks, as well as other configuration parameters, from the RA packets it receives.

Address stateless auto-configuration means that the node automatically configures IPv6 addresses based on the information obtained by router discovery/prefix discovery.

Router discovery/prefix discovery is achieved through RS packets and RA packets.

### **Redirection**

When a host starts up, it may have only one default route to the default gateway in its routing table. When certain conditions are met, the default gateway sends an ICMPv6 redirect packet to the source host, notifying the host to choose a better next-hop for subsequent packets.

### **Configuration Condition**

None

### **Configure IPv6 Static Neighbors.**

Resolving the IPv6 addresses of neighbor nodes to link layer addresses can be achieved either through the address resolution function in the IPv6 ND protocol or by manually configuring static neighbors.

An IPv6 neighbor is uniquely identified by the IPv6 address of the neighbor node and the L3 interface connected to this neighbor node.

Table 43-11 Configuring IPv6 Static Neighbors

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure IPv6 Static Neighbors.	<b>ipv6 neighbor</b> <i>ipv6-address interface-name mac-address</i>	Mandatory By default, no IPv6 static neighbor is configured.

**Configure the Aging Time of IPv6 Neighbor Table Entries in STALE State**

IPv6 neighbor table entries have five reachability states: INCOMPLETE, REACHABLE, STALE, DELAY and PROBE, where the STALE state indicates that it does not know whether the neighbor is reachable or not. The neighbor table entries in the STALE state have an aging time, which will migrate to the DELAY state when reach their aging time.

Table 43-12 Configuring the Aging Time of IPv6 Neighbor Table Entries in STALE State

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the Aging Time of IPv6 Neighbor Table Entries in STALE State	<b>ipv6 neighbor stale-aging</b> <i>aging-time</i>	Optional By default, the aging time of IPv6 neighbor table entry in STALE state is 7200 seconds.

**Configure the retransmission interval of NS packets.**

After the device sends an NS packet, if it does not receive a response within the specified time interval, it will resend the NS packet. The following command allows you to configure the time interval for NS packets retransmission.

Table 43-13 Configuring Time Interval for NS Packets Retransmission

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure time interval for NS packets retransmission.	<b>ipv6 nd ns-interval</b> <i>value</i>	Mandatory  By default, the interface sends NS packets at an interval of 1000 milliseconds.

### Configure the Attempts to Send an NS Packet during the IPv6 Duplicate Address Detection

After the interface is configured with an IPv6 address, it sends a NS packet to request duplicate address detection. If no response is received within a certain period of time, it will keep sending NS packets. When the number of NS packets sent reaches the set value and no response is received, the address is considered available.

Table 43-14 Configuring the Attempts to Send an NS Packet during the IPv6 Duplicate Address Detection

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure the Attempts to Send an NS Packet during the IPv6 Duplicate Address Detection	<b>ipv6 nd dad attempts</b> <i>value</i>	Mandatory  By default, the number of attempts to send an NS packet during the IPv6 duplicate address detection is 1.

### Configure the relevant parameters of RA packets.

Users can configure whether the interface sends RA packets and the time interval for sending RA packets according to the actual situation, and can also configure the relevant parameters in RA packets to notify the host. When the host receives the RA packet, it can use these parameters to operate accordingly.

Table 43-15 Parameters and Descriptions in RA Packets

Parameter	Description
Hop Limit	The host will use the value of this parameter to fill the Hop Limit field in the IPv6 packet header when sending an IPv6 packet. The value of this parameter is also used as the value of the Hop Limit field in the response packet.
MTU	Distributing the link MTU can be used to ensure that all nodes on the same link share the same MTU value.
Router Lifetime	It is used to set the time duration during which the router sending RA packets acts as the default router for the host. Based on the value of the router lifetime parameter in the received RA packet, the host can determine whether to use the router that sent the RA packet as the default router.
Neighbor Reachable Time	When the neighbor reachability is confirmed by neighbor unreachability detection, the device considers the neighbor reachable within the set reachability time. If the device needs to send packets to the neighbor after the set time, it will reconfirm whether the neighbor is reachable.

Table 43-16 Relevant Parameters of RA Packets

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure prefix option information in RA packets.	<b>ipv6 nd prefix</b> { <i>ipv6-prefix</i>   <b>default</b> } [ <i>valid-lifetime</i>   <b>infinite</b>   <b>no-advertise</b>   <b>no-autoconfig</b>   <b>off-link</b> ] [ <i>prefered-lifetime</i>   <b>infinite</b> ]	Mandatory By default, no prefix option information is configured.
Configure the value of the Hop Limit field in the RA packets sent by the interface to be obtained	<b>ipv6 nd ra hop-limit</b>	Optional By default, the value of the Hop Limit field in the RA packets sent by un-

from the global configuration.		configured interfaces is obtained globally, and the value of the Hop Limit field is 0.
Configure the maximum time interval and minimum time interval for sending RA packets.	<b>ipv6 nd ra interval</b> <i>max-value [ min-value ]</i>	Optional By default, the maximum time interval for sending RA packets is 600 seconds and the minimum time interval is 198 seconds.
Configure to enable RA packets to carry the MTU option.	<b>ipv6 nd ra mtu</b>	Optional By default, the RA packets do not carry the MTU option.
Configure router lifetime in the RA packets.	<b>ipv6 nd ra-lifetime</b> <i>value</i>	Optional By default, router lifetime in the RA packets is 1800 seconds.
Forbid the interface from sending RA packets periodically.	<b>ipv6 nd suppress-ra period</b>	Optional By default, RA packets are not sent periodically on the interface.
Forbid the interface from responding to RS packets.	<b>ipv6 nd suppress-ra response</b>	Optional By default, the interface receives RS packets and does not respond to RA packets.

#### Enables the interface to send redirected packets.

After receiving an IPv6 packet that needs forwarding, the device discovers through routing that the receiving interface of the packet is the same as the sending interface, then the device forwards the packet and sends a redirect packet back to the source, notifying the source to re-select the correct next-hop for subsequent packet delivery. By default, the device is able to send redirect packets, but in some specific cases, users can disable the device from sending redirect packets.

Table 43-17 Enable Interface to Send Redirect Packet

Step	Command	Description
------	---------	-------------

Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Enables the interface to send redirected packets.	<b>ipv6 redirects</b>	Optional By default, the interface is enabled to send redirected packets.

#### 43.2.4 Configure to enable the ND fast response function.

##### Configuration Condition

None

##### Configure to Enable the ND Fast Response Function

Table 43-18 Configuring to Enable the ND Fast Response Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure to enable the ND fast response function.	<b>nd fast-response</b>	Mandatory By default, the global ND fast response function is enabled.

#### 43.2.5 Configure L3 Interface ND Proxy.

##### Configuration Condition

None

##### Configure L3 Interface ND Proxy.

Table 43-19 Configuring the L3 ND Proxy Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter L3 interface configuration mode.	<b>interface</b> <i>interface-name</i>	Mandatory After entering the L3 interface configuration mode, subsequent configurations only take effect on the current interface.
Configure L3 interface ND proxy function.	<b>nd proxy enable</b>	Mandatory By default, the proxy function is not enabled on the interface.

### 43.2.6 Configure ICMPv6 functions.

In the IPv6 protocol stack, Internet Control Message Protocol (ICMP) is mainly used to provide network detection services. It also provides an error report if the network layer or transmission layer protocol becomes abnormal, and it informs the related device of the abnormality to facilitate network control management.

#### Configuration Condition

None

#### Configure ICMPv6 error packets transmitting rate.

If an excessive number of ICMPv6 error packets are sent in a short period of time in the network, it may lead to network congestion. To avoid this, users can configure the maximum number of ICMPv6 error packets to be sent within a specified time.

Table 43-20 ICMPv6 Error Packets Transmitting Rate

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure ICMPv6 packets transmitting rate.	<b>ipv6 icmp error-interval</b> <i>interval [ buckets ]</i>	Optional By default, the period for calculating the transmitting rate of ICMPv6 error packets is 100 milliseconds,

		and the maximum number of ICMPv6 error packets sent in the period is 10.
--	--	--

### Enable transmission of ICMPv6 destination unreachable packets.

The ICMPv6 destination unreachable packet sending function allows to discard the IPv6 data packet and send an ICMPv6 destination unreachable error packet to the source if the destination is unreachable after the device receives the IPv6 data packet.

A device sends an ICMPv6 destination unreachable error packet when the following conditions are met:

When forwarding a packet, the device sends a "no route to destination" ICMPv6 error packet to the source if it fails to find a route.

When the device forwards a packet, if the packet cannot be sent because of an administrative policy (e.g., firewall, ACL, etc.), it sends an ICMPv6 error packet that says "Communication with the destination address is prohibited by the administrative policy" to the source.

When the device forwards a packet, if the destination IPv6 address of the packet is out of the range of the source IPv6 address (for example, the source IPv6 address of the packet is a link-local address and the destination IPv6 address of the packet is a global unicast address), the packet will not reach the destination, and an "out of range" ICMPv6 error packet will be sent to the source.

If the device cannot resolve the link layer address corresponding to the destination IPv6 address when forwarding the packet, it sends an "address unreachable" ICMPv6 error packet to the source.

When the device receives an IPv6 packet with a local destination address and UDP transport layer protocol, if the destination port number of the packet does not match the process in use, it sends a "port unreachable" ICMPv6 error packet to the source.

Since the information delivered to the user process by the ICMPv6 destination unreachable error packet is unreachable, it may affect the normal use of the end user if there is a malicious attack. To avoid the above situation, users can disable the ICMPv6 destination unreachable error packet sending function of the device.

Table 43-21 Enable Transmission of ICMPv6 Destination Unreachable Packets

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Enable transmission of ICMPv6 destination unreachable packets.	<b>ipv6 unreachable</b>	Optional  By default, the function of sending ICMPv6 destination unreachable packet is enabled.
--	-------------------------	---

### 43.2.7 Configure TCP anti-attack function for IPv6.

The IPv6 TCP server receives a large number of SYN packets but the peer end does not respond to the SYN-ACK response from the server. This can cause the server's memory to be consumed heavily, taking up the server's syn queue and causing the IPv6 TCP server unable to service normal requests. Such attacks can be avoided by configuring IPv6 TCP anti-attack function.

#### Configuration Condition

None

#### Enable the IPv6 TCP Syncache Function

This function does not rush to allocate the TCB when a SYN data packet is received, but first responds with a SYN+ACK packet and stores this half-open connection information in a dedicated cache until a correct response ACK packet is received before allocating the TCB.

Table 43-22 Enable the IPv6 TCP Syncache Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable the IPv6 TCP Syncache Function	<b>ipv6 tcp syncache</b>	Mandatory  By default, the IPv6 TCP syncache function is disabled.

#### Enable the IPv6 TCP Syncookies Function

This function does not use any storage resources at all, it uses a special algorithm to generate Sequence Number. The algorithm takes into account fixed information including the other party's IPv6, port, its own IPv6 and port, and other fixed information of its own, such as MSS, time, etc. After receiving the other party's ACK packet, the algorithm will recalculate it to see if it is the same as the other party's response packet (Sequence Number-1), so as to decide whether to allocate TCB resources.

Table 43-23 Enable the IPv6 TCP Syncookies Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable the IPv6 TCP Syncookies Function	<b>ipv6 tcp syncookies</b>	Mandatory  By default, the IPv6 TCP syncookies function is disabled.

### 43.2.8 IPv6 Basic Monitoring and Maintaining

Table 43-24 IPv6 Basic Monitoring and Maintaining

Command	Description
<b>clear nd fast-response statistics</b>	The command is used to clear the ND fast response statistics.
<b>clear ipv6 icmp6stat</b>	Clears the ICMPv6 statistics.
<b>clear ipv6 interface statistics</b>	Clears the interface IPv6 packet statistics.
<b>clear ipv6 mtu</b>	Clears the IPv6 path MTU information.
<b>clear ipv6 neighbors</b>	Clears the IPv6 dynamic neighbor table entries.
<b>clear ipv6 statistics</b>	Clears the IPv6 basic statistics.
<b>clear ipv6 tcp syncache statistics</b>	Clears the IPv6 TCP protocol syncache statistics.
<b>clear ipv6 tcp6stat</b>	Clears the IPv6 TCP statistics.
<b>clear ipv6 udp6stat</b>	Clears the IPv6 UDP statistics.
<b>show nd fast-response statistics</b>	The command is used to display the ND fast response statistics.
<b>show ipv6 hop-limit</b>	Displaying the IPv6 global Hop Limit values.

Command	Description
<b>show ipv6 frag-queue</b>	Displaying the cached IPv6 fragment packets.
<b>show ipv6 icmp6state</b>	Displaying the ICMPv6 statistics.
<b>show ipv6 interface</b>	Displaying the interface IPv6 information.
<b>show ipv6 interface statistics</b>	Displaying the interface IPv6 statistics.
<b>show ipv6 max-mtu</b>	Displaying the maximum value of IPv6 MTU currently supported by the system.
<b>show ipv6 mtu</b>	Displaying the IPv6 path MTU information.
<b>show ipv6 neighbors</b>	Displaying the IPv6 neighbor information.
<b>show ipv6 prefix</b>	Displaying the IPv6 address prefix information.
<b>show ipv6 sockets</b>	Displaying the IPv6 socket information.
<b>show ipv6 statistics</b>	Displaying the basic IPv6 statistics.
<b>show ipv6 tcp syncache detail</b>	Displaying the IPv6 TCP protocol syncache table entry information.
<b>show ipv6 tcp syncache statistics</b>	Displaying the IPv6 TCP protocol syncache statistics.
<b>show ipv6 tcp6state</b>	Displaying the IPv6 TCP statistics.
<b>show ipv6 udp6state</b>	Displaying the IPv6 UDP statistics.

## 43.3 Basic Configuration Example of IPv6

### 43.3.1 Configure the IPv6 Address of an Interface

#### Network Requirements

- The two devices are connected via Ethernet interfaces, and the interfaces are configured with IPv6 global unicast addresses to verify Interoperability between them.

#### Network Topology



Figure 43-1 Network Topology for Configuring the IPv6 Address of an Interface

### Configuration Steps

Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Enable the IPv6 forwarding function of the device.

#### #Configure Device1.

```
Device1#configure terminal
Device1(config)#ipv6 unicast-routing
```

#### #Configure Device2.

```
Device2#configure terminal
Device2(config)#ipv6 unicast-routing
```

Step 3: Configure the global unicast address of the interface.

#### #Configure the global unicast address of Device1 interface vlan 2 as 2001:1::1/64.

```
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#ipv6 address 2001:1::1/64
Device1(config-if-vlan2)#exit
```

#### #Configure the global unicast address of Device2 interface vlan 2 as 2001:1::2/64.

```
Device2(config)#interface vlan 2
Device2(config-if-vlan2)#ipv6 address 2001:1::2/64
Device2(config-if-vlan2)#exit
```

Step 4: Check the result.

#### #Check the interface details of Device1.

```
Device1#show ipv6 interface vlan 2
vlan2 is up
VRF: global
IPv6 is enable, link-local address is fe80::201:7aff:fe46:a64d
Global unicast address(es):
  2001:1::1, subnet is 2001:1::/64
Joined group address(es):
  ff02::1:ff00:1
  ff02::1:ff00:0
  ff02::2
  ff02::1
  ff02::1:ff46:a64d
ND control flags: 0x1
MTU is 1500 bytes
ICMP redirects are enabled
ICMP unreachable are enabled
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 (unspecified)
ND advertised retransmit interval is 0 (unspecified)
ND MaxRtrAdvInterval is 600
ND MinRtrAdvInterval is 198
ND AdvDefaultLifetime is 1800
```

After the IPv6 address is configured, the IPv6 protocol function is automatically enabled on the interface, and the link-local address is automatically generated and added to the corresponding multicast group.

#### #Check the interface details of Device2.

```
Device2#show ipv6 interface vlan 2
vlan2 is up
VRF: global
IPv6 is enable, link-local address is fe80::201:7aff:fe22:e222
Global unicast address(es):
  2001:1::2, subnet is 2001:1::/64
Joined group address(es):
  ff02::1:ff00:2
  ff02::1:ff00:0
  ff02::2
  ff02::1
  ff02::1:ff22:e222
ND control flags: 0x1
MTU is 1500 bytes
ICMP redirects are enabled
ICMP unreachable are enabled
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 (unspecified)
ND advertised retransmit interval is 0 (unspecified)
ND MaxRtrAdvInterval is 600
ND MinRtrAdvInterval is 198
ND AdvDefaultLifetime is 1800
```

#### #On Device1, Ping the link-local address fe80::0201:7aff:fe22:e222 of Device2.

```
Device1#ping fe80::0201:7aff:fe22:e222

Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to fe80::201:7aff:fe22:e222 , timeout is 2 seconds:

Output Interface: vlan 2
!!!!
Success rate is 100% (5/5). Round-trip min/avg/max = 0/96/483 ms.
```

---

### Note

- When pinging the link-local address, you need to specify the output interface, which is an interface on the same link as the pinged link-local address.

---

#### #On Device1, Ping the global unicast address 2001:1::2 of Device2.

```
Device1#ping 2001:1::2

Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 2001:1::2 , timeout is 2 seconds:
!!!!
Success rate is 100% (5/5). Round-trip min/avg/max = 0/36/183 ms.
```

Device1 and Device2 can communicate with each other.

---

## 43.3.2 Configuring IPv6 Neighbor Discovery

### Network Requirements

- Device and the PC belong to the same LAN.
- Interface VLAN2 of Device is configured with EUI-64 address.
- The PC obtains an IPv6 address prefix through the IPv6 neighbor discovery protocol and automatically configures an IPv6 address based on the obtained address prefix. Implement IPv6 protocol communication between the PC and Device.

### Network Topology

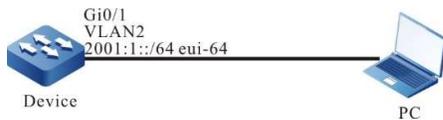


Figure 43-2 Network Topology for Configuring IPv6 Neighbor Discovery

### Configuration Steps

Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Enable the IPv6 forwarding function of the device.

```
Device#configure terminal
Device(config)#ipv6 unicast-routing
```

Step 3: Configure EUI-64 unicast address and enable RA advertisement function.

#Device's vlan2 is configured with EUI-64 address to enable the RA advertisement function of vlan2.

```
Device(config)#interface vlan 2
Device(config-if-vlan 2)#ipv6 address 2001:1::/64 eui-64
Device(config-if-vlan 2)#no ipv6 nd suppress-ra period
Device(config-if-vlan 2)#no ipv6 nd suppress-ra response
Device(config-if-vlan 2)#exit
```

---

### Note

- By default, the RA advertisement function is disabled.
- 

#Check the interface details of Device.

```
Device#show ipv6 interface vlan 2
vlan2 is up
VRF: global
IPv6 is enable, link-local address is fe80::201:7aff:fe5d:e7d3
```

```

Global unicast address(es):
  2001:1::201:7aff:fe5d:e7d3, subnet is 2001:1::/64 [EUI]
Joined group address(es):
  ff02::1:ff00:0
  ff02::2
  ff02::1
  ff02::1:ff5d:e7d3
ND control flags: 0x85
MTU is 1500 bytes
ICMP redirects are enabled
ICMP unreachable are enabled
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 (unspecified)
ND advertised retransmit interval is 0 (unspecified)
ND MaxRtrAdvInterval is 600
ND MinRtrAdvInterval is 198
ND AdvDefaultLifetime is 1800

```

#### Step 4: Configure the PC.

#IPv6 protocol is installed on the PC. The configuration of IPv6 varies by operating system, and the Windows XP is used here as an example.

```

C:\>ipv6 install
Installing...
Succeeded.

```

#### Step 5: Check the result.

#Check the interface details of PC.

```

C:\>ipconfig
..... (omitted)
Ethernet adapter 130:

    Connection-specific DNS Suffix  .:
    IP Address. . . . . : 130.255.128.100
    Subnet Mask . . . . . : 255.255.0.0
    IP Address. . . . . : 2001:1::15b3:d4:f13d:c3da
    IP Address. . . . . : 2001:1::3a83:45ff:feef:c724
    IP Address. . . . . : fe80::3a83:45ff:feef:c724%6
    Default Gateway . . . . . : fe80::201:7aff:fe5e:cfc1%6

```

It can be seen that after the PC obtains the IPv6 address prefix 2001:1::/64, and the global unicast address is automatically generated according to this prefix.

---

### Note

- The Windows XP host obtains the address prefix and generates two global unicast addresses, one of which has an interface ID generated based on the MAC address of the interface, and the other has a randomly generated interface ID.
- 

#On Device, ping the link-local address fe80::3a83:45ff:feef:c724 of the PC.

```
Device#ping fe80::3a83:45ff:feef:c724
```

Press key (ctrl + shift + 6) interrupt it.

---

Sending 5, 76-byte ICMP Echos to fe80::3a83:45ff:feef:c724 , timeout is 2 seconds:

Output Interface: vlan2  
!!!!  
Success rate is 100% (5/5). Round-trip min/avg/max = 0/29/149 ms.

#On Device, ping the global unicast address 2001:1::15b3:d4:f13d:c3da and 2001:1::3a83:45ff:feef:c724 automatically generated on the PC.

Device#ping 2001:1::15b3:d4:f13d:c3da  
  
Press key (ctrl + shift + 6) interrupt it.  
Sending 5, 76-byte ICMP Echos to 2001:1::15b3:d4:f13d:c3da , timeout is 2 seconds:  
!!!!  
Success rate is 100% (5/5). Round-trip min/avg/max = 0/36/183 ms.

Device#ping 2001:1::3a83:45ff:feef:c724  
  
Press key (ctrl + shift + 6) interrupt it.  
Sending 5, 76-byte ICMP Echos to 2001:1::3a83:45ff:feef:c724 , timeout is 2 seconds:  
!!!!  
Success rate is 100% (5/5). Round-trip min/avg/max = 0/26/133 ms.

The PC and Device can communicate with each other.

---

## Note

- When pinging the link-local address, you need to specify the output interface, which is an interface on the same link as the pinged link-local address.
- 

### 43.3.3 Configure L3 ND Proxy

#### Network Requirements

- Device is directly connected to PC1 and PC2 respectively. The network prefixes where PC1 and PC2 are located are the same, both are 2001:1:1::/48.
- The interface VLAN2 of Device has a MAC address of 0001.7a6a.01f0.
- Through the L3 ND proxy of Device, PC1 is able to ping through to PC2, and PC1 can learn PC2's MAC address.

#### Network Topology

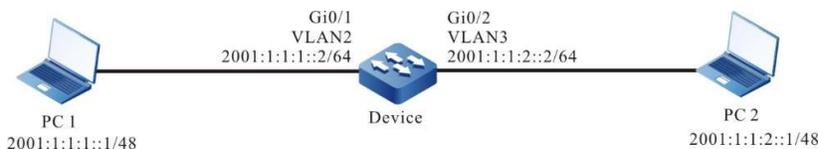


Figure 43-3 Network Topology for Configuring L3 ND Proxy

#### Configuration Steps

Step 1: Configure Virtual Local Area Networks (VLANs), and add ports to the required VLANs. (Omitted)

Step 2: Configure IP addresses for the ports. (Omitted)

Step 3: Configure L3 ND Proxy.

#Enable L3 ND proxy under the L3 interface VLAN2 of Device.

```
Device(config)#interface vlan 2
Device(config-if-vlan2)#nd proxy enable
Device(config-if-vlan2)#exit
```

#Enable L3 ND proxy under the L3 interface VLAN3 of Device.

```
Device(config)#interface vlan 3
Device(config-if-vlan3)#nd proxy enable
Device(config-if-vlan3)#exit
```

Step 4: Check the results.

#PC1 ping PC2 with the address 2001:1:1:2::1.

```
C:\Documents and Settings>ping 2001:1:1:2::1
```

```
Pinging 2001:1:1:2::1 with 32 bytes of data:
Reply from 2001:1:1:2::1: bytes=32 time=997ms TTL=255
Reply from 2001:1:1:2::1: bytes=32 time<1ms TTL=255
Reply from 2001:1:1:2::1: bytes=32 time<1ms TTL=255
Reply from 2001:1:1:2::1: bytes=32 time<1ms TTL=255
Ping statistics for 2001:1:1:2::1
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 997ms, Average = 249ms
```

#Check the neighbor table entries of Device.

```
Device#sh ipv6 neighbors
IPv6 Address      Age Link-layer Addr  flags  State Interface
2001:1:1:1::1    0  00e0.4c6b.f753  405   STALE  vlan2
2001:1:1:2::1    1  0857.00da.4715  405   STALE  vlan3
```

#Check the neighbor table entries of PC1.

```
C:\Documents and Settings>netsh interface ipv6 show neighbors
Internet Address      Physical Address  Type
-----
2001:1:1:1::2        00-01-7a-6a-01-f0  Stale (Router)
2001:1:1:2::1        00-01-7a-6a-01-f0  Stale (Router)
```

#PC1 is able to ping through to PC2, and PC1 learns the neighbor table entry of PC2. The MAC address in the neighbor table entry is the MAC address of VLAN2 0001.7a6a.01f0.



---

---

The device does not have L3 ND proxy enabled by default.

---

# 44 DHCPv6

---

## 44.1 Overview

It is hard to manage a large network. For example, in a network in which IPv6 addresses are manually allocated, IPv6 address conflicts are common. The only way of solving the problem is to dynamically allocate IPv6 addresses to the hosts. The Dynamic Host Configuration Protocol version 6 (DHCPv6) allocates the IPv6 address to requesting hosts from an address pool. DHCPv6 also provides other information, such as DNS server address. DHCPv6 reduces the workload of the administrator in recording and tracking manually allocated IPv6 addresses.

DHCPv6 is a protocol that is based on UDP broadcast. The process for a DHCPv6 client to obtain an IPv6 address and other configuration information from the DHCPv6 server contains four phases.

**SOLICIT phase.** When the DHCPv6 client accesses the network for the first time, it sends a DHCP SOLICIT packet with the source address as the client's linklocal address and the destination address as ff02::1:2.

**ADVERTISE phase.** When the DHCPv6 server receives the DHCP SOLICIT broadcast packet from the client, it will select an IPv6 address from the corresponding address pool according to the policy and send it to the client together with other parameters via the DHCP ADVERTISE packet.

**REQUEST phase.** If the DHCPv6 client receives responses from multiple DHCPv6 servers on the network, it will pick only one of them, i.e. DHCP ADVERTISE, (usually the first one to arrive), and will send a DHCP REQUEST packet to the network, telling all DHCPv6 servers which server it will accept the IPv6 address from.

In the **REPLY phase**, when the DHCPv6 server receives a DHCP REQUEST packet from a DHCPv6 client, it sends a DHCP REPLY acknowledgment packet to the DHCPv6 client containing its provided IPv6 address and other configurations, telling the DHCPv6 client that it can use the IPv6 address it provided.

The IPv6 addresses allocated by DHCPv6 server to DHCPv6 clients have a lease, and the DHCPv6 server will take back the allocated IPv6 addresses after it expires. When the IPv6 address lease of a DHCPv6 client is half remaining, the DHCPv6 client sends a DHCP ENEW packet to the DHCPv6 server to renew its IPv6 lease. If the DHCPv6 client can continue to use the IPv6 address, the DHCPv6 server responds to the DHCP REPLY packet to notify the DHCPv6 client to renew the lease; if the DHCPv6 client cannot continue to use the IPv6 address, the DHCPv6 server does not respond.

Since the request packet is sent in multicast mode during the dynamic acquisition of IPv6 address, DHCPv6 is only applicable when the DHCPv6 client and DHCPv6 server are in the same subnet. If there are multiple subnets in a network and the hosts of multiple subnets need to provide IPv6 addresses and other configuration information through DHCPv6 servers, the hosts of these subnets can communicate with DHCPv6 servers through DHCPv6 relay devices to obtain IPv6 addresses and other configuration information.

## 44.2 DHCPv6 Function Configuration

Table 44-1 DHCPv6 Function Configuration List

Configuration Task	
Configure a DHCPv6 address pool	Create a DHCPv6 address pool that allows you to specify VRF attributes.
	Configure the IPv6 address range
	Configure a DNS server address.
	Configure the IPv6 address lease
	Configure to bind IPv6 with DUID and IAID.
Configure other parameters of the DHCPv6 server.	Configure the DHCPv6 Server.
	Configure the ranges of the reserved IPv6 address.
	Configure the DHCPv6 ping probe parameters.
	Configure the data logging function of the DHCPv6 server.
Configure the function of DHCPv6 client	Configure DHCPv6 client
	Configure the function of DHCPv6 Option 16
Configure the function of DHCPv6 relay	Configure DHCPv6 relay.
	Configure the source address of DHCPv6 relay packet.
	Configure DHCPv6 server address

	Configure DHCPv6 interface-id option
--	--------------------------------------

## 44.2.1 Configure a DHCPv6 address pool

### Configuration Condition

None

### Create a DHCPv6 Address Pool

The DHCPv6 server selects and allocates IPv6 addresses and other related parameters for clients from the DHCPv6 address pool, therefore, the DHCPv6 server must first create a DHCPv6 address pool.

Table 44-2 Creating a DHCPv6 Address Pool

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Create a DHCPv6 address pool and enter the DHCPv6 configuration mode.	<b>ipv6 dhcp pool <i>pool-name</i> [ vrf <i>vrf-name</i> ]</b>	Mandatory By default, the DHCPv6 address pool is not created by the system.

### Note

- Address pools fall into two types: Network and Range. The two types of address pools can be configured respectively through the network and range commands.

### Configure the IPv6 address range

On the DHCPv6 server, each DHCPv6 address pool should be configured with the corresponding IPv6 address range to allocate IPv6 addresses to DHCPv6 clients.

Table 44-3 Configuring IPv6 Address Ranges

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Enter the DHCPv6 configuration mode.	<b>ipv6 dhcp pool</b> <i>pool-name</i> [ <b>vrf</b> <i>vrf-name</i> ]	-
Configure the ranges of Network-type IPv6 addresses.	<b>network</b> <i>ipv6-address/prefix-length</i>	Optional By default, the address pool is not configured with an IPv6 address range.
Configure the ranges of Range-type IPv6 addresses.	<b>range</b> <i>low-ipv6-address high-ipv6-address prefix-length</i>	Optional By default, the address pool is not configured with an IPv6 address range.

### Note

- Change the type of the address pool from network to range (or vice versa). If the address range of the new configuration and the address range of the old configuration intersect, the command line will prompt the user whether to perform this operation, if yes, any relevant address configurations (static binding) and dynamic leases under the address pool will be deleted; if the actual effective address range of the new configuration covers the actual effective address range of the old configuration, the address pool will keep all relevant address configurations under the address pool (static binding). However, it will delete the dynamic lease.

### Configure a DNS server address.

On a DHCPv6 server, you can configure the DNS server address respectively for each DHCPv6 address pool. When a DHCPv6 server allocates an IPv6 address for a DHCPv6 client, it also sends the DNS server address to the client.

When the DHCPv6 client starts dynamic domain name resolution, it queries the DNS server.

Table 44-4 Configuring a DNS Server Address

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the DHCPv6 configuration mode.	<b>ipv6 dhcp pool</b> <i>pool-name</i> [ <b>vrf</b> <i>vrf-name</i> ]	-

Configure a DNS server address.	<b>dns-server</b> { <i>ipv6-address</i> &<1-8> / <b>autoconfig</b> }	Mandatory  By default, the DNS server address is not configured.
---------------------------------	--	--

### Configure the IPv6 address lease

The IPv6 address that the DHCPv6 server allocates to the DHCPv6 client has a lease. After the lease expires, the server will take back the allocated IPv6 address. If the DHCPv6 client wants to continue to use the address, it must have the IPv6 address lease updated.

On the DHCPv6 server, you can configure the IPv6 address lease time for each DHCPv6 address pool separately.

Table 44-5 Configuring Ipv6 Address Lease Time

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the DHCPv6 configuration mode.	<b>ipv6 dhcp pool</b> <i>pool-name</i> [ <b>vrf</b> <i>vrf-name</i> ]	-
Configure the IPv6 address lease	<b>lease preferred-lifetime</b> <i>preferred-lifetime</i> <b>valid-lifetime</b> <i>valid-lifetime</i>	Mandatory  By default, the <b>preferred-lifetime</b> is 604800 seconds (7 days) and the <b>valid-lifetime</b> is 2592000 seconds (30 days).

### Configure to bind IPv6 with DUID and IAID.

Configure to bind IPv6 with the client's DUID and IAID. When the client with specified DUID and IAID requests the DHCPv6 server to allocate IPv6 address, the DHCPv6 server will assign its bound IPv6 address. As long as the DUID and IAID of this client remain unchanged, the IPv6 address the client obtains from the server will remain the same every time.

Table 44-6 Configuring to Bind IPv6 with DUID and IAID

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Enter the DHCPv6 configuration mode.	<b>ipv6 dhcp pool</b> <i>pool-name</i> [ <b>vrf</b> <i>vrf-name</i> ]	-
Configure to bind IPv6 with DUID and IAID.	<b>bind</b> <i>ipv6-address</i> <b>duid</b> <i>duid</i> [ <b>iaid</b> { <i>iaid</i>   <b>decimal</b> <i>iaid</i> } ]	Mandatory By default, IPv6 is not configured to bind with DUID and IAID.

### Note

- This command is valid only for Range-type and Network-type address pools.
- When configuring static binding for the same DUID and IAID, the address pool allows binding of five IPv6 addresses.
- The configured static binding specifies only the DUID, and when the IAID is not specified, the address pool allows only one IPv6 address to be bound.

## 44.2.2 Configure other parameters of the DHCPv6 server.

### Configuration Condition

None

### Configure the DHCPv6 Server.

After configuring the interface to work in DHCPv6 server mode, when the interface receives DHCPv6 request packets from DHCPv6 clients, the DHCPv6 server allocates IPv6 addresses and other network parameters for the clients.

Table 44-7 Configuring DHCPv6 Server

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure DHCPv6 server function.	<b>ipv6 dhcp server</b>	Mandatory By default, the DHCPv6 server

		function is not configured.
--	--	-----------------------------

### Configure the ranges of the reserved IPv6 address.

In the DHCPv6 address pool, some IPv6 addresses are reserved for specific devices, and some are in conflict with other host IPv6 addresses on the network. Therefore, these IPv6 addresses cannot be used for dynamic allocation.

Table 44-8 Configuring the Ranges of Reserved IPv6 Addresses

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the ranges of the reserved IPv6 address.	<b>ipv6 dhcp excluded-address</b> <i>low-ipv6-address</i> [ <i>high-ipv6-address</i> ] [ <b>vrf</b> <i>vrf-name</i> ]	Mandatory  By default, the range of the reserved IPv6 address is not configured.  The IPv6 addresses within the reserved IPv6 address ranges do not participate in address allocation.

### Configure DHCPv6 Ping Probe Parameters

To prevent IPv6 address conflict, the DHCPv6 server needs to detect the IPv6 address before dynamically allocating it to the DHCPv6 client. The detection is performed by a ping operation, which determines whether there is an IPv6 address conflict based on the detection of whether an ICMPv6 echo response packet can be received within a specified time.

Table 44-9 Configuring DHCPv6 Ping Probe Parameters

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the DHCPv6 ping probe parameters.	<b>ipv6 dhcp ping</b> { <b>packets</b> <i>packet-num</i>   <b>timeout</b> <i>milliseconds</i> }	Mandatory  By default, the number of ping packets is 1, and the timeout time is 500 ms.

### Configure the Data Logging Function of the DHCPv6 Server

When the data log function of a DHCPv6 server is enabled, the address pool allocation on the DHCPv6 server will be recorded to the data log.

Table 44-10 Configuring DHCPv6 Server Data Logging Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the data logging function switch of DHCPv6 server.	<b>ipv6 dhcp logging security-data</b>	Mandatory By default, the data logging function is not enabled.

### 44.2.3 Configure the function of DHCPv6 client

#### Configuration Condition

None

#### Configure DHCPv6 client

The interface of DHCPv6 client can obtain IPv6 address and other parameters through DHCPv6.

Table 44-11 Configuring DHCPv6 Clients

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface <i>interface-name</i></b>	-
Configure DHCPv6 Clients to Obtain IPv6 Addresses.	<b>ipv6 dhcp client address [ rapid-commit ]</b>	Mandatory By default, the DHCPv6 client request for IPv6 address is not configured.
Configure DHCPv6 clients to obtain IPv6 prefixes.	<b>ipv6 dhcp client pd <i>pool-name</i> [ rapid-commit ]</b>	Mandatory By default, the DHCPv6 client request for IPv6 prefix is not configured.

---

## 44.2.4 Configure the function of DHCPv6 relay

### Configuration Condition

None

### Configure DHCPv6 relay.

If there are multiple subnets in a network and the hosts of multiple subnets need to provide IPv6 addresses and other configuration information through DHCPv6 servers, the hosts of these subnets can communicate with DHCPv6 servers through DHCPv6 relay devices to obtain IPv6 addresses and other configuration information. If an interface is configured to work in DHCPv6 relay mode, after the interface receives DHCPv6 packets from a DHCPv6 client, it relays the packet to the specified DHCPv6 server. The DHCPv6 server then allocates an IPv6 address.

Table 44-12 Configuring DHCPv6 Relay

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure the function of DHCPv6 relay	<b>ipv6 dhcp relay</b>	Mandatory By default, the DHCPv6 relay function is not configured.

### Configure the source address of DHCPv6 relay packet.

The source address used by DHCPv6 relay when forwarding DHCPv6 client-originated packets to a DHCPv6 server is, by default, the output interface address of the route to the DHCPv6 server. In some environments, the DHCPv6 server cannot communicate with this address, therefore users are allowed to configure the source address of the packets forwarded by the DHCPv6 relay to the DHCPv6 server and the LinkAddr field in the packets via the **ipv6 dhcp relay source-address** command.

Table 44-13 Configuring DHCPv6 Relay Packets Source Address

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure the source address of DHCPv6 relay packet.	<b>ipv6 dhcp relay source-address</b> <i>ipv6-address</i>	Mandatory By default, the DHCPv6 relay packet source address is not configured.

### Configure DHCPv6 server address

After the interface receives DHCPv6 packets from a DHCPv6 client, it relays the packet to the specified DHCPv6 server. The DHCPv6 server then allocates an IPv6 address.

Table 44-14 Configuring DHCPv6 Server Address

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure DHCPv6 server address	<b>ipv6 dhcp relay server -address</b> <i>ipv6-address</i>	Mandatory By default, the DHCPv6 server address is not configured.

### Configure DHCPv6 interface-id option

This command is used to configure the interface-id option fill mode supported by DHCPv6 relay.

Table 44-15 Configuring DHCPv6 Server Address

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure DHCPv6 interface-id option	<b>ipv6 dhcp relay interface -id [ interface   user-define</b> <i>defined-string</i> <b>]</b>	Mandatory By default, the interface-id option fill mode is not configured.

## Configure DHCPv6 Remote-id Option

This command is used to configure the fill mode of the remote-id option supported by DHCPv6 relay.

Table 44-16 Configuring DHCPv6 Server Address

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure DHCPv6 Remote-id Option	<b>ipv6 dhcp relay remote-id user-define</b> <i>defined-string</i>	Mandatory By default, the fill mode of the remote-id option is not configured.

## 44.2.5 DHCPv6 Monitoring and Maintaining

Table 44-17 DHCPv6 Monitoring and Maintaining

Command	Description
<b>clear ipv6 dhcp pool</b> <i>pool-name</i> { <b>lease</b>   <b>conflict</b> [ <i>ipv6-address</i> ] }	Clears dynamic lease information from the address pool or address information with conflicting addresses.
<b>clear ipv6 dhcp server interface</b> [ <i>interface-name</i> ] <b>statistics</b>	Clears the key statistics when the DHCPv6 server interacts with clients or relays for packets.
<b>clear ipv6 dhcp relay statistics</b>	Clear the statistics on the DHCPv6 relay device.
<b>show ipv6 dhcp server interface</b> <i>interface-name</i> [ <b>statistics</b> ]	Displaying the address pool information associated with the specified interface or display the key statistics when the DHCPv6 server engages in packet interactions with clients or relays under the specified interface.
<b>show ipv6 dhcp pool</b> <i>pool-name</i> { <b>summary</b>   <b>ping_list</b>   <b>offer_list</b>	Displaying the summary information of the specified address pool or the information of

<b>excluded_list   conflict_list   lease   binding }</b>	the address that is doing ping check or the address that has sent the OFFER packet and is waiting for the DHCPv6 client to respond to the REQUEST packet or the information of the excluded address in the address pool or the information of the address that has address conflict in the address pool or the information of dynamic lease in the address pool or the information of static binding in the address pool.
<b>show ipv6 dhcp pool <i>pool-name</i> specific { ipv6-address <i>ipv6-address</i>   duid <i>duid</i> }</b>	Displaying information about the specified ip address or client DUID in the address pool.
<b>show ipv6 dhcp relay [interface <i>interface-name</i> ]</b>	Displaying the packet statistics on the DHCPv6 relay device.

## 44.3 Typical Configuration Example of DHCPv6

### 44.3.1 Configure the DHCPv6 server to statically allocate IPv6 addresses.

#### Network Requirements

- Device2 acts as the DHCPv6 server and statically allocates the IPv6 address and DNS server IPv6 address to the client.
- The DHCPv6 server allocates IPv6 address to PC1 with DUID binding and PC2 with DUID+IAID binding.

#### Network Topology

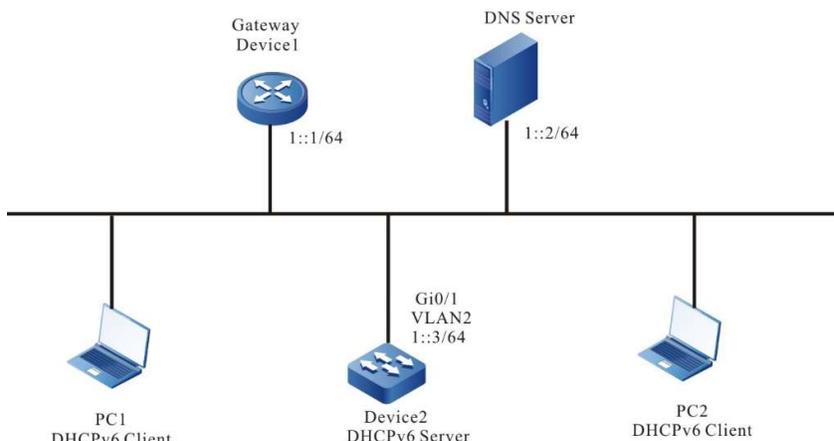


Figure 44-1 Network Topology for Configuring DHCPv6 Server to Statically Allocate IPv6 Addresses

### Configuration Steps

Step 1: Configure the IPv6 address for the Device2 interface and the DHCPv6 server.

```
Device2#configure terminal
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ipv6 address 1::3/64
Device2(config-if-vlan2)#ipv6 dhcp server
Device2(config-if-vlan2)#exit
```

Step 2: Configure statically bound address pools and parameters.

#Configure address pool binding and uses static DUID binding to allocate IPv6 address to PC1. Use static DUID+IAID binding to allocate IPv6 address to PC2.

```
Device2(config)#ipv6 dhcp pool binding
Device2(dhcp6-config)#bind 1::11 duid 000200001613303030313761636635646634
Device2(dhcp6-config)#bind 1::12 duid 000200001613636364383166313037616239 iaid 00010071
Device2(dhcp6-config)#dns-server 1::2
Device2(dhcp6-config)#exit
```

Step 3: Check the result.

#Check the association of the server interfaces and the addresses.

```
Device2#show ipv6 dhcp server interface vlan2
DHCPv6 server status information:
DHCP server is enabled on interface: vlan2
Vrf : global
```

```
DHCPv6 server pool information:
Available directly-connected pool:
  Interface IP: 1::1/64
  Pool name: binding
  Range:
    min: 101::
    max: 101::ffff:ffff:ffff:ffff
  utilization: 0.00%
```

#Check the static binding of the server.

```
Device2#show ipv6 dhcp pool binding binding
IPv6 Address      Duid              Iaid  Type  Time Left(s)
-----
1::11  000200001613303030313761636635646634  00000000  Binding  NA
1::12  000200001613636364383166313037616239  00010071  Binding  NA
```

#Check the IPv6 addresses allocated to PC1 and PC2 on Device2 with the show ipv6 dhcp pool binding lease command.

```
Device2#show ipv6 dhcp pool mac-binding lease
IPv6 Address      Duid              Iaid  Type  Time Left(s)
-----
1::11  000200001613303030313761636635646634  00000000  Lease  2591974
1::12  000200001613636364383166313037616239  00010071  Lease  2591974
```

Check on PC1 and PC2 that the obtained IPv6 address, and the DNS server IPv6 address is correct.

### 44.3.2 Configure DHCPv6 server to dynamically allocate IPv6 addresses.

#### Network Requirements

- The two interfaces vlan2 and vlan3 of Device are configured with IPv6 addresses 1::3/64 and 2::3/64 respectively.
- The DHCPv6 server Device dynamically allocates IPv6 addresses to the 1::/64 and 2::/64 network segments for clients within each of the two directly connected physical networks.
- Addresses within network segment 1::/64 are leased for 1 day with a DNS server address of 2::4; addresses within network segment 2::/64 are leased for 3 days with a gateway address of 2::3 and a DNS server address of 2::4.
- The first 10 IPv6 addresses in network segment 1::/64 and network segment 2::/64 are reserved and cannot be allocated.

#### Network Topology

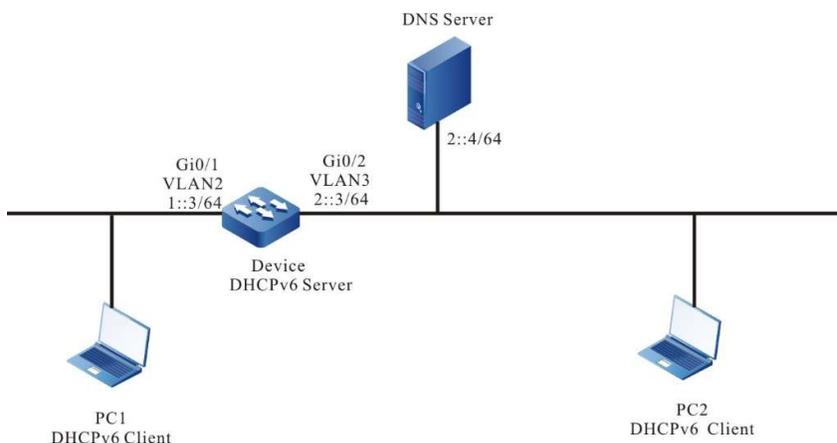


Figure 44-2 Network Topology for Configuring DHCPv6 to Dynamically Allocate IPv6 Addresses

#### Configuration Steps

- Step 1: Configure VLANs, and add ports to the required VLANs. Configure IPv6 addresses for the ports. (Omitted)
- Step 2: On the DHCPv6 server Device1, configure two dynamic address pools and their parameters.

#Configure the DHCPv6 server.

```
Device(config)#interface vlan2
Device(config-if-vlan2)#ipv6 dhcp server
Device(config-if-vlan2)#exit
Device(config)#interface vlan3
Device(config-if-vlan3)#ipv6 dhcp server
Device(config-if-vlan3)#exit
```

---

#Configure the first 10 IPv6 addresses in the two address pools to be reserved.

```
Device(config)#ipv6 dhcp excluded-address 1::0 1::9
Device(config)#ipv6 dhcp excluded-address 2::0 2::9
```

#Configure address pool dynamic-pool1 and its parameters (including address range, DNS, address lease, and local domain name).

```
Device(config)#ipv6 dhcp pool dynamic-pool1
Device(dhcp6-config)#network 1::/64
Device(dhcp6-config)#dns-server 2::4
Device(dhcp6-config)#lease preferred-lifetime 86300 valid-lifetime 86400
Device(dhcp6-config)#exit
```

#Configure address pool dynamic-pool2 and its parameters (including address range, DNS address, address lease, Wins server address, and local domain name).

```
Device(config)#ip DHCPv6 pool dynamic-pool2
Device(dhcp6-config)#network 2::/64
Device(dhcp6-config)#dns-server 2::4
Device(dhcp6-config)#lease preferred-lifetime 259100 valid-lifetime 259200
Device(dhcp6-config)#exit
```

Step 3: Check the result.

#Check the IPv6 address information allocated to the client on the Device.

```
Device#show ipv6 dhcp pool dynamic-pool1 lease
IPv6 Address      Duid              Iaid  Type    Time Left(s)
-----
1::a      000200001613303030313761636635646634  00000000  Lease    86390
Device2#show ipv6 dhcp pool dynamic-pool2 lease
IPv6 Address      Duid              Iaid  Type    Time Left(s)
-----
2::a      000200001613303030313761636635646634  00000000  Lease    2591974
```

Check if the IPv6 address is obtained correctly on the DHCPv6 client.

---

注意：

- The IPv6 addresses in the address pool must be within the network segment range of the interface that provides the service.
- 

### 44.3.3 Configure DHCPv6 relay.

#### Network Requirements

- Device1 is the DHCPv6 server and Device2 interface is enabled for DHCPv6 relay function.
- The DHCPv6 server serves clients in the 1::/64 network segment, and the first 10 IPv6 addresses are reserved.
- The DHCPv6 client obtains IPv6 addresses through the DHCPv6 relay.

#### Network Topology

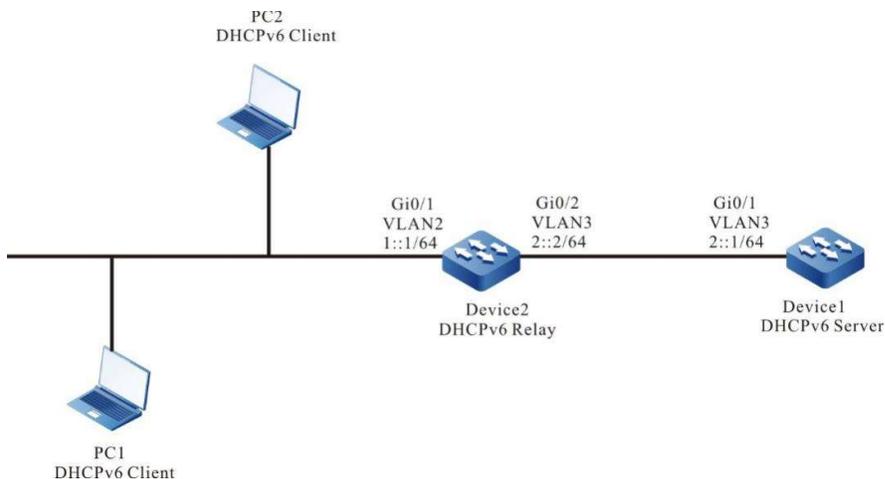


Figure 44-3 Network Topology for Configuring DHCPv6 Relay

### Configuration Steps

Step 1: Configure VLANs, and add ports to the required VLANs. Configure the IPv6 address of each interface (omitted).

Step 2: Configure Device1's IPv6 address pool and reserved IPv6 addresses.

#Configure Device1 as the DHCPv6 server.

```
Device1#configure terminal
Device1(config)#interface vlan3
Device2(config-if-vlan3)#ipv6 dhcp server
Device2(config-if-vlan3)#exit
```

#Configure to ensure the IPv6 addresses from 1::0 to 1::9 cannot be allocated.

```
Device1(config)#ipv6 dhcp excluded-address 1::0 1::9
```

# Configure the IPv6 address pool dynamic-pool of Device1.

```
Device1(config)#ipv6 dhcp pool dynamic-pool
Device1(dhcp6-config)#network 1::/64
Device1(dhcp6-config)#lease preferred-lifetime 300 valid-lifetime 600
Device1(dhcp6-config)#exit
```

#Configure a static route to network segment 1::/64.

```
Device1(config)#ipv6 route 1::0/64 2::2
```

Step 3: Enable the DHCPv6 relay and configure DHCPv6 server address 2::1 on the vlan2 interface of Device2.

```
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ipv6 dhcp relay
Device2(config-if-vlan2)#ipv6 dhcp relay server-address 2::1
Device2(config-if-vlan2)#exit
```

Step 4: Check the result.

#Check the IPv6 address information allocated on Device1.

```
Device1#show ipv6 dhcp pool dynamic-pool lease
IPv6 Address      Duid      Iaid      Type      Time Left(s)
-----
```

Using the `show ipv6 dhcp pool dynamic-pool lease` command to view information about the IPv6 address allocated to the client, indicating that the client has acquired IPv6 address 1::0.

# 45 GRE

---

## 45.1 Overview

GRE (Generic Routing Encapsulation), is a generic tunnel encapsulation protocol that specifies how one network protocol can be used to encapsulate another network protocol.

GRE tunneling, one of many tunneling technologies, requires manual configuration of the start and end points of the tunnel, which is a virtual point-to-point connection that provides a transmission channel for encapsulated packets, with encapsulation and decapsulation of data packets at each end of the tunnel.

- Generic Routing Encapsulation

When a data packet is to be sent through a GRE tunnel, the tunnel adds a GRE header to its header, and an IP header before the GRE header. The protocol number in the IP header is set to 47 (the protocol number of the GRE protocol in the IP header), the source address in the IP header is set as the source address of the tunnel, and the destination address in the IP header is set as the destination address of the tunnel.

- GRE Packet Structure

Delivery header	GRE header	Payload packet
-----------------	------------	----------------

**Payload packet:** Refers to the network layer packet (e.g. IP packets) before entering the tunnel. As the payload of tunnel packets, the protocol of this packet is called the passenger protocol of the GRE tunnel.

**GRE header:** Refers to the GRE header added after the Payload packet enters the tunnel, which contains the GRE protocol itself and some information related to the passenger protocol.

**Delivery header:** The encapsulated external protocol header (e.g., IP header), i.e., the protocol header of the network in which the tunnel is located, is the transmission tool that enables packets of one protocol to traverse another protocol network.

- GRE Packet Forwarding

After the packet is encapsulated at the start of the GRE tunnel, it is routed according to the encapsulated destination address and then sent out from the corresponding network interface. The intermediate device forwards it as a normal packet until it reaches the end of the tunnel.

- Generic Routing Decapsulation

The decapsulation process is the opposite of the encapsulation process. The tunnel endpoint receives the packet and analyzes the delivery header first. If the destination address is its own address, the protocol field in the IP header will be checked, and if the protocol field is 47 (GRE protocol number), the packet is handed over to the GRE tunnel for processing. The tunnel first removes the delivery header, then checks the GRE header for protocol number, checksum, keywords, etc. After completing the corresponding processing, the GRE header is removed, and then the Payload packet is handed over to the passenger protocol for subsequent processing to complete the decapsulation.

## 45.2 GRE Function Configuration

Table 45-1 GRE Function Configuration List

Configuration Task	
Configure GRE tunnels.	Configuring GRE over IPv4 tunnels.
	Configuring GRE over IPv6 tunnels.

### 45.2.1 Configure GRE tunnels.

#### Configuration Condition

Before configuring GRE tunnels, ensure that

- Configuring the interface IP address to make it reachable at the network layer of adjacent nodes.
- Create the tunnel interface and configure the basic parameters (refer to the tunnel interface configuration manual).
- Configure any unicast routing protocol to make routes reachable at both ends of the tunnel.

#### Configure GRE tunnels.

Table 45-2 Configuring GRE Tunnels

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the tunnel interface configuration mode.	<b>interface tunnel</b> <i>tunnel-number</i>	-
Configure tunnel interface addresses.	Configure IPv4 unicast addresses. <b>ip address</b> <i>ip-address</i> { <i>mask</i>   <i>mask-length</i> }	Mandatory  By default, the tunnel interface address is not configured.
	Configure an IPv6 global unicast address or anycast address or site-local address or auto-acquire address. <b>ipv6 address</b> { <i>ipv6-address/prefix-length</i> [ <i>anycast</i>   <i>eui-64</i> ]   <b>autoconfig</b> }	
	Configure IPv6 link-local addresses. <b>ipv6 address</b> <i>IPv6-address</i> <b>link-local</b>	Optional  By default, the link-local address is automatically generated when IPv6 is enabled on the interface.
Configure the tunnel interface mode as GRE over IPv4 or GRE over IPv6.	<b>tunnel mode gre</b> [ <b>ip</b>   <b>ipv6</b> ]	Optional  By default, the tunnel interface mode is GRE over IPv4.
Configure the tunnel interface source address or interface name.	<b>tunnel source</b> { <i>ip-address</i>   <i>ipv6-address</i>   <i>interface-name</i> }	Mandatory  By default, the tunnel interface is not configured with source address and interface name.
Configure the destination address or host name of the tunnel interface.	<b>tunnel destination</b> { <i>ip-address</i>   <i>ipv6-address</i> }	Mandatory

Step	Command	Description
		By default, the tunnel interface is not configured with destination address.

### Note

- The source and destination addresses must be configured on both ends of the tunnel, and the addresses on both ends must be the source and destination addresses of each other.
- When configuring the tunnel source, if the interface method is used, the primary address of the source interface is taken as the source address of the tunnel.
- Both ends of the tunnel should be configured to the same tunnel mode, otherwise transmission through the tunnel will fail.
- Two or more tunnels with the same tunnel mode, source address, and destination address cannot be configured at the same time on the same device.

## 45.2.2 GRE Monitoring and Maintaining

Table 45-3 GRE Monitoring and Maintaining

Command	Description
<b>enable</b>	Privileged mode
<b>debug tunnel {all   config   event   forward   packet }</b>	Enable the Tunnel debugging information switch
<b>show tunnel [tunnel-id] [slot slot-num]</b>	Displaying tunnel information

## 45.3 Typical Configuration Example of GRE

### 45.3.1 Configure Basic Functions of GRE

#### Network Requirements

- IP Network1 and IP Network2 are the two private networks of Device1 and Device3 respectively.

- IP Network1 and IP Network2 communicate through a GRE tunnel between Device1 and Device3.

## Network Topology

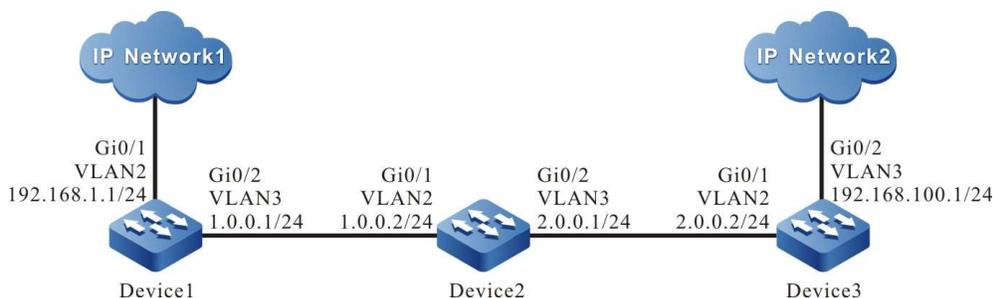


Figure 45-1 Network Topology for Configuring Basic Functions of GRE

## Configuration Steps

Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configure IP addresses for the ports. (Omitted)

Step 3: Configure OSPF.

### #Configure Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#network 1.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#exit
```

### #Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 1.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#exit
```

### #Configure Device3.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#exit
```

### #Check the routing table of Device3.

```
Device3#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS
```

Gateway of last resort is not set

```
O 1.0.0.0/24 [110/65536] via 2.0.0.1, 00:18:40, vlan2
C 2.0.0.0/24 is directly connected, 00:22:27, vlan2
C 192.168.100.0/24 is directly connected, 00:00:28, vlan3
```

---

 **Note**

- Device1 and Device2 are checked in the same way as Device3, the process of which is omitted.
- 

Step 4: Configure GRE tunnels.

#Configure GRE tunnel1 on Device1 with source address 1.0.0.1, destination address 2.0.0.2 and IP address 10.0.0.1.

```
Device1(config)#interface tunnel 1
Device1(config-if-tunnel1)#tunnel source 1.0.0.1
Device1(config-if-tunnel1)#tunnel destination 2.0.0.2
Device1(config-if-tunnel1)#ip address 10.0.0.1 255.255.255.0
Device1(config-if-tunnel1)#exit
```

#Configure GRE tunnel1 on Device3 with source address 2.0.0.2, destination address 1.0.0.1 and IP address 10.0.0.2.

```
Device3(config)#interface tunnel 1
Device3(config-if-tunnel1)#tunnel source 2.0.0.2
Device3(config-if-tunnel1)#tunnel destination 1.0.0.1
Device3(config-if-tunnel1)#ip address 10.0.0.2 255.255.255.0
Device3(config-if-tunnel1)#exit
```

#Check information about the GRE tunnel on Device3.

```
Device3#show tunnel 1
Tunnel 1:
  Tunnel mode is gre ip
  Gre checksum validation is disabled
  Gre key is not set
  Gre keepalive is disabled
  Source ipv4 address is 2.0.0.2(Source ipv4 address is up on source interface vlan2)
  Destination ipv4 address is 1.0.0.1
  Tunnel state is up
  Encapsulation vrf is global(0x0)
  TTL(time-to-live) is 255
  TOS(type of service) is not set
total(1)
```

---

 **Note**

- Device1 is checked in the same way as that of Device3, the process of which is omitted.
  - When the tunnels are not in the same network segment, you need to configure static routes on the devices at both ends of a local tunnel to reach a peer tunnel, and the output interface is configured as the interface of the local tunnel.
-

---

Step 5: Configure static routes.

#On Device1, configure a static route to the IP Network2 with the output interface as tunnel1.

```
Device1(config)#ip route 192.168.100.0 255.255.255.0 tunnel1
```

#On Device3, configure a static route to the IP Network1 with the output interface as tunnel1.

```
Device3(config)#ip route 192.168.1.0 255.255.255.0 tunnel1
```

#Check the routing table of Device3.

```
Device3#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

O  1.0.0.0/24 [110/65536] via 2.0.0.1, 00:43:30, vlan2
C  2.0.0.0/24 is directly connected, 00:47:17, vlan2
C  10.0.0.0/24 is directly connected, 00:17:12, tunnel1
S  192.168.1.0/24 [1/100000] is directly connected, 00:00:10, tunnel1
```

---

## Note

- Device1 is checked in the same way as that of Device3, the process of which is omitted.
- 

## 45.3.2 Configure Basic Functions of GRE Over IPv6

### Network Requirements

- IP Network1 and IP Network2 are the private IP networks of Device1 and Device3 respectively.
- IPv6 Network1 and IPv6 Network2 are the private IPv6 networks of Device1 and Device3 respectively.
- IP Network1 and IP Network2 communicate through a GRE over IPv6 tunnel between Device1 and Device3.
- IPv6 Network1 and IPv6 Network2 communicate through a GRE over IPv6 tunnel between Device1 and Device3.

### Network Topology

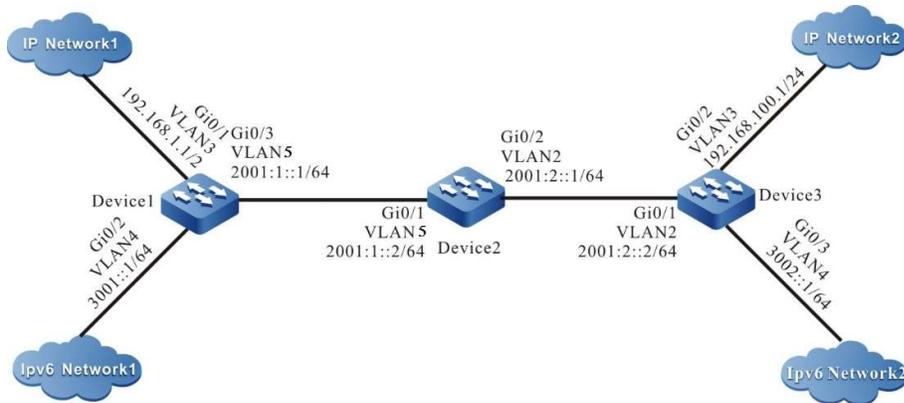


Figure 45-2 Network Topology for Configuring Basic Functions of GRE

### Configuration Steps

Step 1: Configure IP addresses for the ports. (Omitted)

Step 2: Configure OSPFv3 to enable communication between Device1, Device2, and Device3.

#### #Configure Device1.

```
Device1#configure terminal
Device1(config)#ipv6 router ospf 100
Device1(config-ospf6)#router-id 1.1.75.1
Device1(config-ospf6)#exit
Device1(config)#interface vlan5
Device1(config-if-vlan5)#ipv6 router ospf tag 100 area 0
Device1(config-if-vlan5)#exit
```

#### #Configure Device2.

```
Device2#configure terminal
Device2(config)#ipv6 router ospf 100
Device2(config-ospf6)#router-id 1.2.75.1
Device2(config-ospf6)#exit
Device2(config)#interface vlan5
Device2(config-if-vlan5)#ipv6 router ospf tag 100 area 0
Device2(config-if-vlan5)#exit
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ipv6 router ospf tag 100 area 0
Device2(config-if-vlan2)#exit
```

#### #Configure Device3.

```
Device3#configure terminal
Device3(config)#ipv6 router ospf 100
Device3(config-ospf6)#router-id 1.1.73.1
Device3(config-ospf6)#exit
Device3(config)#interface vlan2
Device3(config-if-vlan2)#ipv6 router ospf tag 100 area 0
Device3(config-if-vlan2)#exit
```

#### # Check the IPv6 routing table of Device3.

```
Device3#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
U - Per-user Static route
O - OSPF, OE-OSPF External, M - Management
```

---

```
L ::1/128 [0/0]
  via ::, 6w0d:23:09:31, lo0
O 2001:1::/64 [110/2]
  via fe80::508b:fff:fee4:ff6, 00:08:37, vlan2
C 2001:2::/64 [0/0]
  via ::, 00:15:51, vlan2
L 2001:2::2/128 [0/0]
  via ::, 00:15:50, lo0
C 3002::/64 [0/0]
  via ::, 00:15:06, vlan4
L 3002::1/128 [0/0]
  via ::, 00:15:04, lo0
```

---

## Note

- Device1 and Device2 are checked in the same way as Device3, the process of which is omitted.
- 

Step 3: Configure GRE over IPv6 tunnels.

#Configure GRE over IPv6 tunnel1 on Device1, with the source address 2001:1::1, destination address 2001:2::2, IP address 10.0.0.1, and IPv6 address 10::1.

```
Device1(config)#interface tunnel 1
Device1(config-if-tunnel1)#tunnel mode gre ipv6
Device1(config-if-tunnel1)#tunnel source 2001:1::1
Device1(config-if-tunnel1)#tunnel destination 2001:2::2
Device1(config-if-tunnel1)#ip address 10.0.0.1 255.255.255.0
Device1(config-if-tunnel1)#ipv6 address 10::1/64
Device1(config-if-tunnel1)#exit
```

#Configure GRE over IPv6 tunnel1 on Device3, with the source address 2001:2::2, destination address 2001:1::1, IP address 10.0.0.2, and IPv6 address 10::2.

```
Device3(config)#interface tunnel 1
Device3(config-if-tunnel1)#tunnel mode gre ipv6
Device3(config-if-tunnel1)#tunnel source 2001:2::2
Device3(config-if-tunnel1)#tunnel destination 2001:1::1
Device3(config-if-tunnel1)#ip address 10.0.0.2 255.255.255.0
Device3(config-if-tunnel1)#ipv6 address 10::2/64
Device3(config-if-tunnel1)#exit
```

#Check information about the GRE tunnel on Device3.

```
Device3#show tunnel 1
```

```
Tunnel 1:
  Tunnel mode is gre ipv6
  Gre checksum validation is disabled
  Gre key is not set
  Source ipv6 address is 2001:2::2(Source ipv6 address is up on source interface gigabitethernet0/2/0)
  Destination ipv6 address is 2001:1::1
  Tunnel state is up
  Encapsulation vrf is global(0x0)
  TTL(time-to-live) is 255
  TOS(type of service) is not set
total(1)
```

 **Note**

- Device1 is checked in the same way as that of Device3, the process of which is omitted.
- When the tunnels are not in the same network segment, you need to configure static routes on the devices at both ends of a local tunnel to reach a peer tunnel, and the output interface is configured as the interface of the local tunnel.

Step 4: Configure static routes.

#On Device1, configure a static route to the IP Network2 with the output interface as tunnel1.

```
Device1(config)#ip route 192.168.100.0 255.255.255.0 tunnel1
```

#On Device1, configure a static route to the IPv6 Network2 with the output interface as tunnel1.

```
Device1(config)#IPv6 route 3002::/64 tunnel1
```

#On Device3, configure a static route to the IP Network1 with the output interface as tunnel1.

```
Device3(config)#ip route 192.168.1.0 255.255.255.0 tunnel1
```

#On Device3, configure a static route to the IPv6 Network1 with the output interface as tunnel1.

```
Device3(config)#IPv6 route 3001::/64 tunnel1
```

#Check the routing table of Device3.

```
Device3#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS
```

Gateway of last resort is not set

```
C 10.0.0.0/24 is directly connected, 00:17:12, tunnel1
S 192.168.1.0/24 [1/100000] is directly connected, 00:00:10, tunnel1
C 192.168.100.0/24 is directly connected, 00:00:28, vlan3
```

# Check the IPv6 routing table of Device3.

```
Device3#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management
```

```
L ::1/128 [0/0]
   via ::, 6w0d:23:50:28, lo0
C 10::/64 [0/0]
   via ::, 00:12:23, tunnel1
L 10::2/128 [0/0]
   via ::, 00:12:22, lo0
O 2001:1::/64 [110/2]
   via fe80::508b:fff:fee4:ff6, 00:49:34, vlan2
C 2001:2::/64 [0/0]
   via ::, 00:56:48, vlan2
```

---

L 2001:2::2/128 [0/0]  
via ::, 00:56:46, lo0  
S 3001::/64 [1/100000]  
via ::, 00:00:14, tunnel1  
C 3002::/64 [0/0]  
via ::, 00:56:02, vlan4  
L 3002::1/128 [0/0]  
via ::, 00:56:01, lo0

---

 **Note**

- Device1 is checked in the same way as that of Device3, the process of which is omitted.
-

# 46 IPIP Tunnel

---

## 46.1 Overview

IPIP (IPv4 over IPv4) tunneling, one of many tunneling technologies, is similar to GRE (Generic Routing Encapsulation) tunneling in that the start and end points of the tunnel need to be manually configured. It is a virtual point-to-point connection that provides a transmission channel for encapsulated packets, with encapsulation and decapsulation of data packets at each end of the tunnel. IPIP tunnels, which encapsulate only IPv4 data packets so that these encapsulated data packets can be transmitted in another IPv4 network.

- IPIP Encapsulation

When an IP data packet is to be sent through an IPIP tunnel, the tunnel adds an IP packet header with the protocol number set to 4 in the IP packet header, the source address in the IP packet header is set to the source address of the tunnel, and the destination address in the IP packet header is set to the destination address of the tunnel.

- IPIP Packet Structure



**IP Payload:** The IP packet load before entering the tunnel, as the payload of the tunnel packet.

**IP header:** the first part of the IP packet before entering the tunnel.

**Outer IP header:** The encapsulated external IP packet header, which is a transport tool to enable IP packets to traverse another IP network.

- IPIP Packet Forwarding

After the packet is encapsulated at the start of the IPIP tunnel, it is routed according to the encapsulated destination address and then sent out from the corresponding network interface. The intermediate device forwards it as a regular IP packet until it reaches the end of the tunnel.

- IPIP Decapsulation

The decapsulation process is the opposite of the encapsulation process. The tunnel endpoint receives the packet and analyzes the outer IP header first. If the destination address is its own address, the protocol field in the IP header will be checked, and if the protocol field is 4, the packet is handed over to the IPIP tunnel for processing. After the tunnel removes the Outer IP header of the packet, it performs routing based on the destination address of the decapsulated packet and performs subsequent processing based on the routing result.

## 46.2 IPIP Function Configuration

Table 46-1 IPIP Function Configuration List

Configuration Task	
Configure IPIP tunnels.	Configure IPIP tunnels.

### 46.2.1 Configure IPIP tunnels.

#### Configuration Condition

Before configuring IPIP tunnels, ensure that

- Configuring the interface IP address to make it reachable at the network layer of adjacent nodes.
- Create the tunnel interface and configure the basic parameters (refer to the tunnel interface configuration manual).
- Configure any unicast routing protocol or static route to make both ends of the tunnel reachable via route.

#### Configure IPIP tunnels.

Table 46-2 Configuring IPIP Tunnels

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the tunnel interface configuration mode.	<b>interface tunnel <i>tunnel-number</i></b>	-

Step	Command	Description
Configure tunnel interface addresses.	<b>ip address</b> <i>ip-address</i> { <i>mask</i>   <i>mask-length</i> }	Mandatory By default, the tunnel interface address is not configured.
Configure the tunnel interface mode as IPv4 over IPv4.	<b>tunnel mode ipip</b>	Mandatory By default, the tunnel interface mode is GRE over IPv4.
Configure the tunnel interface source address or interface name.	<b>tunnel source</b> { <i>ip-address</i>   <i>interface-name</i> }	Mandatory By default, the tunnel interface is not configured with source address and interface name.
Configure the destination address or host name of the tunnel interface.	<b>tunnel destination</b> { <i>ip-address</i> }	Mandatory By default, the tunnel interface is not configured with destination address.

## Note

- The tunnel interface address needs to be configured with an IPv4 address, and the passenger protocol can only be an IPv4 protocol.
- The source and destination addresses must be configured on both ends of the tunnel, and the addresses on both ends must be the source and destination addresses of each other.
- When configuring the tunnel source, if the interface method is used, the primary address of the source interface is taken as the source address of the tunnel.
- Both ends of the tunnel should be configured to the same tunnel mode, otherwise transmission through the tunnel will fail.
- Two or more tunnels with the same tunnel mode, source address, and destination address cannot be configured at the same time on the same device.

## 46.2.2 IPIP Monitoring and Maintaining

Refer to GRE Monitoring and Maintenance in Section 7.2.2 of the GRE Configuration Manual.

## 46.3 Typical Configuration Example of IPIP Tunnel

### 46.3.1 Configure IPIP Basic Functions

#### Network Requirements

- IP Network1 and IP Network2 are the two private networks of Device1 and Device3 respectively.
- IP Network1 and IP Network2 communicate through a IPIP tunnel between Device1 and Device3.

#### Network Topology

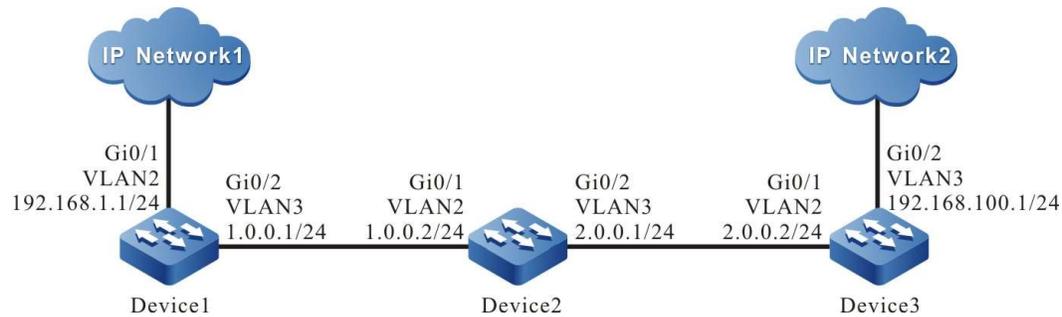


Figure 8-1 Network Topology for Configuring Basic Functions of IPIP

#### Configuration Steps

Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configure IP addresses for the ports. (Omitted)

Step 3: Configure OSPF.

#### #Configure Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#network 1.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#exit
```

#### #Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 1.0.0.0 0.0.0.255 area 0
```

```
Device2(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#exit
```

### #Configure Device3.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#exit
```

### #Check the routing table of Device3.

```
Device3#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS
```

Gateway of last resort is not set

```
O 1.0.0.0/24 [110/65536] via 2.0.0.1, 00:18:40, v1an2
C 2.0.0.0/24 is directly connected, 00:22:27, v1an2
C 192.168.100.0/24 is directly connected, 00:00:28, v1an3
```

---

## Note

- Device1 and Device2 are checked in the same way as Device3, the process of which is omitted.
- 

### Step 4: Configure IPIP tunnels.

#### #Configure IPIP tunnel1 on Device1 with source address 1.0.0.1, destination address 2.0.0.2 and IP address 10.0.0.1.

```
Device1(config)#interface tunnel 1
Device1(config-if-tunnel1)#tunnel mode ipip
Device1(config-if-tunnel1)#tunnel source 1.0.0.1
Device1(config-if-tunnel1)#tunnel destination 2.0.0.2
Device1(config-if-tunnel1)#ip address 10.0.0.1 255.255.255.0
Device1(config-if-tunnel1)#exit
```

#### #Configure IPIP tunnel1 on Device3 with source address 2.0.0.2, destination address 1.0.0.1 and IP address 10.0.0.2.

```
Device3(config)#interface tunnel 1
Device3(config-if-tunnel1)#tunnel mode ipip
Device3(config-if-tunnel1)#tunnel source 2.0.0.2
Device3(config-if-tunnel1)#tunnel destination 1.0.0.1
Device3(config-if-tunnel1)#ip address 10.0.0.2 255.255.255.0
Device3(config-if-tunnel1)#exit
```

#### #Check information about the IPIP tunnel on Device3.

```
Device3#show tunnel 1
Tunnel 1:
Tunnel mode is ipip
```

```
Source ipv4 address is 2.0.0.2(Source ipv4 address is up on source interface vlan2)
Destination ipv4 address is 1.0.0.1
Tunnel state is up
Encapsulation vrf is global(0x0)
TTL(time-to-live) is 255
TOS(type of service) is not set
total(1)
```

---

## Note

- Device1 is checked in the same way as that of Device3, the process of which is omitted.
  - When the tunnels are not in the same network segment, you need to configure static routes on the devices at both ends of a local tunnel to reach a peer tunnel, and the output interface is configured as the interface of the local tunnel.
- 

Step 5: Configure static routes.

#On Device1, configure a static route to the IP Network2 with the output interface as tunnel1.

```
Device1(config)#ip route 192.168.100.0 255.255.255.0 tunnel1
```

#On Device3, configure a static route to the IP Network1 with the output interface as tunnel1.

```
Device3(config)#ip route 192.168.1.0 255.255.255.0 tunnel1
```

#Check the routing table of Device3.

```
Device3#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

O  1.0.0.0/24 [110/65536] via 2.0.0.1, 00:43:30, vlan2
C  2.0.0.0/24 is directly connected, 00:47:17, vlan2
C  10.0.0.0/24 is directly connected, 00:17:12, tunnel1
S  192.168.1.0/24 [1/100000] is directly connected, 00:00:10, tunnel1
```

---

## Note

- Device1 is checked in the same way as that of Device3, the process of which is omitted.
-

# 47 Transition Tunnel

## 47.1 Overview

Transition tunneling (IPv6 over IPv4) technology provides a way to deliver IPv6 data with the existing IPv4 routing system: IPv6 packets are encapsulated in IPv4 packets as unstructured meaningful data for transmission over IPv4 networks. Depending on the creation method, transition tunnels can be divided into two categories: manually configured tunnels and automatically configured tunnels. The transition tunneling technique makes clever use of existing IPv4 networks, and is significant in that it provides a way to enable communication between IPv6 nodes during the transition, however it does not solve the problem of interoperability between IPv6 and IPv4 nodes. Transition tunnels are divided into two types, i.e. manual and automatic. The correspondences between its types and modes are shown in the following table.

Table 47-1 Transition Tunnel Modes

Tunnel types	Tunnel modes	Tunnel source/destination address	Tunnel interface address
Manually configured tunnels	Manually configured IPv6 over IPv4 tunnels	The source/destination address is a manually configured IPv4 address.	IPv6 address
Automatically configured tunnels	6to4 tunnels		6to4 address in the format: 2002:a.b.c.d::/48
	ISATAP tunnels		ISATAP address in the format: Prefix:0:5EFE:a.b.c.d/64

- Manually configured IPv6 over IPv4 tunnels

This type of tunnel is established by manual configuration, and the endpoint address of the tunnel is determined by the configuration without allocating a

special IPv6 address to the node, and is suitable for use between IPv6 nodes that communicate frequently.

- 6to4 tunnels

The 6to4 tunnel is a point-to-multipoint tunnel. Both ends of the tunnel require a special IPv6 address in the format: 2002:a.b.c.d::/48, where 2002 indicates a fixed IPv6 address prefix and a.b.c.d indicates the globally unique 32-bit IPv4 address corresponding to the 6to4 tunnel. The tunnel encapsulation process automatically uses this embedded IPv4 address as the end point of the tunnel, which largely simplifies the creation of tunnels. Therefore, nodes using the 6to4 mechanism must have at least one globally unique IPv4 address, and this mechanism is suitable for communication between nodes running IPv6. Since the first 48 bits of the 6to4 IPv6 address prefix are already determined by a fixed value and the IPv4 address, the remaining 16 bits of the subnet number can be defined by the user, which allows more flexibility in interconnecting IPv6 networks using IPv4 networks. The 6to4 tunnels overcome the limitations of using automatically configured IPv4 over IPv6 tunnels.

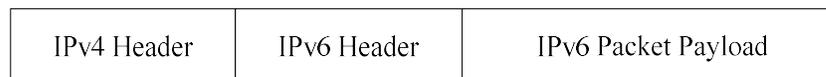
- ISATAP tunnels

ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) tunnels are point-to-multipoint automatic tunnels that require a special IPv6 address at both ends of the tunnel in the format of Prefix:0:5EFE:a.b.c.d/64, where Prefix stands for any legal IPv6 unicast address prefix, and a.b.c.d stands for a 32-bit IPv4 address (not required to be globally unique). This embedded IPv4 address is automatically used as the endpoint of the tunnel during tunnel encapsulation. Therefore, the ISATAP tunnel is also automatically created.

- Transition Tunnel Encapsulation

When an IPv6 data packet is to be sent through an transition tunnel, the tunnel adds an IP packet header with the protocol number set to 41 in the IP packet header, the source address in the IP packet header is set to the source address of the tunnel, and the destination address in the IP packet header is set according to the tunnel type: if it is a manually configured tunnel it is set to the configured tunnel destination address, if it is an automatically configured tunnel it uses the IPv4 address embedded in the IPv6 address.

- Transition Tunnel Packet Structure



IPv6 Packet Payload: The IPv6 packet load before entering the tunnel, acting as the payload of the tunnel packet.

IPv6 Header: The header of the IPv6 packet before entering the tunnel.

IPv4 Header: The encapsulated outer IPv4 header, which is the transport tool that enables IPv6 packets to traverse the IPv4 network.

- Transition Tunnel Packet Forwarding

After the packet is encapsulated at the start of the transition tunnel, it is routed according to the encapsulated destination address and then sent out from the corresponding network interface. The intermediate device forwards it as a regular IP packet until it reaches the end of the tunnel.

- Transition Tunnel Decapsulation

The decapsulation process is the opposite of the encapsulation process. The tunnel endpoint receives the packet and analyzes the IPv4 header first. If the destination address is its own address, the protocol field in the IP header will be checked, and if the protocol field is 41, the packet is handed over to the transition tunnel for processing. After the tunnel removes the IPv4 IP header of the packet, it performs routing based on the destination address of the decapsulated packet and performs subsequent processing based on the routing result.

## 47.2 Transition Tunnels Function Configuration

Table 47-2 Transition Tunnels Function Configuration List

Configuration Task	
Transition tunnels configuration	Manually configure IPv6 over IPv4 tunnels
	Configure 6to4 tunnels
	Configure ISATAP tunnels

### Note

- For configuration commands related to transition tunnels, refer to the IP Tunnels chapter in the User Manual.

### 47.2.1 Manually configure IPv6 over IPv4 tunnels

#### Configuration Condition

Before manually configuring IPv6 over IPv4 tunnels, ensure that

- Configure the physical interface IP address so that adjacent nodes are reachable at the network layer.
- Create the tunnel interface and configure the basic parameters (refer to the tunnel interface configuration manual).
- Configure any unicast routing protocol to make routes reachable at both ends of the tunnel.

### Manually configure IPv6 over IPv4 tunnels

Table 47-3 Manually Configure IPv6 Over IPv4 Tunnels

Step	Command	Description	
Enter the global configuration mode.	<b>configure terminal</b>	-	
Enter the tunnel interface configuration mode.	<b>interface tunnel <i>tunnel-number</i></b>	-	
Configure tunnel interface addresses.	Configure an IPv6 global unicast address or anycast address or site-local address or auto-acquire address.	<b>ipv6 address { <i>ipv6-address/prefix-length</i> [ <i>anycast</i>   <i>eui-64</i> ]   <b>autoconfig</b> }</b>	Mandatory By default, the tunnel interface is not configured with IPv6 address.
	Configure IPv6 link-local addresses.	<b>ipv6 address <i>ipv6-address</i> link-local</b>	Optional By default, the link-local address is automatically generated when IPv6 is enabled on the interface.
Configure the tunnel interface mode as manually configured IPv6 over IPv4 tunnels.	<b>tunnel mode ipv6ip</b>	Mandatory By default, the tunnel interface mode is GRE over IPv4.	

Step	Command	Description
Configure the tunnel interface source address or interface name.	<b>tunnel source</b> { <i>ip-address</i>   <i>interface-name</i> }	Mandatory  By default, the tunnel interface is not configured with source address and interface name.
Configure the destination address or host name of the tunnel interface.	<b>tunnel destination</b> { <i>ip-address</i>   <i>hostname</i> }	Mandatory  By default, the tunnel interface is not configured with destination address and host name.

---

### Note

- The source and destination addresses must be configured on both ends of the tunnel, and the addresses on both ends must be the source and destination addresses of each other.
  - When configuring the tunnel source, if the interface method is used, the primary address of the source interface is taken as the source address of the tunnel.
  - Both ends of the tunnel should be configured to the same tunnel mode, otherwise transmission through the tunnel will fail.
  - Multiple tunnels with the same tunnel mode, source address and destination address cannot be configured at the same time on the same device.
- 

## 47.2.2 Configure 6to4 tunnels

### Configuration Condition

Before configuring 6to4 tunnels, ensure that

- Configure the physical interface IP address so that adjacent nodes are reachable at the network layer.
- Create the tunnel interface and configure the basic parameters (refer to the tunnel interface configuration manual).
- Configure any unicast routing protocol to make routes reachable at both ends of the

tunnel.

## Configure 6to4 tunnels

Table 47-4 Configuring 6to4 Tunnels

Step	Command	Description	
Enter the global configuration mode.	<b>configure terminal</b>	-	
Enter the tunnel interface configuration mode.	<b>interface tunnel <i>tunnel-number</i></b>	-	
Configure tunnel interface addresses.	Configure an IPv6 global unicast address or anycast address or site-local address or auto-acquire address.	<b>ipv6 address { <i>ipv6-address/prefix-length</i> [ <i>anycast</i>   <i>eui-64</i> ]   <i>autoconfig</i> }</b>	Mandatory  By default, the tunnel interface is not configured with IPv6 address.
	Configure IPv6 link-local addresses.	<b>ipv6 address <i>ipv6-address</i> link-local</b>	Optional  By default, the link-local address is automatically generated when IPv6 is enabled on the interface.
Configure the tunnel interface mode as 6to4.	<b>tunnel mode ipv6ip 6to4</b>	Mandatory  By default, the tunnel interface mode is GRE over IPv4.	
Configure the tunnel interface source address or interface name.	<b>tunnel source { <i>ip-address</i>   <i>interface-name</i> }</b>	Mandatory  By default, the tunnel interface is not configured with source address and interface name.	

Step	Command	Description
Configure the tunnel interface to reference the reflection group.	<b>tunnel service-loop</b> <i>service-loop-id</i>	Mandatory By default, the tunnel interface does not reference the reflection group.

---

### Note

- The 6to4 tunnel does not need to be configured with a destination break address; the destination address used for tunnel encapsulation is automatically obtained from the IPv4 address embedded in the IPv6 address of the 6to4 tunnel.
  - When configuring the tunnel source, if the interface method is used, the primary address of the source interface is taken as the source address of the tunnel.
  - Both ends of the tunnel should be configured to the same tunnel mode, otherwise transmission through the tunnel will fail.
  - Only one 6to4 tunnel can be configured on the device.
- 

## 47.2.3 Configure ISATAP tunnels

### Configuration Condition

Before configuring the ISATAP tunnel, ensure that

- Configure the physical interface IP address so that adjacent nodes are reachable at the network layer.
- Create the tunnel interface and configure the basic parameters (refer to the tunnel interface configuration manual).
- Configure any unicast routing protocol to make routes reachable at both ends of the tunnel.

### Configure ISATAP tunnels

Table 47-5 Configuring ISATAP Tunnels

Step	Command	Description	
Enter the global configuration mode.	<b>configure terminal</b>	-	
Enter the tunnel interface configuration mode.	<b>interface tunnel</b> <i>tunnel-number</i>	-	
Configure tunnel interface addresses.	Configure an IPv6 global unicast address or anycast address or site-local address or auto-acquire address.	<b>ipv6 address</b> { <i>ipv6-address/prefix-length</i> [ <b>anycast</b>   <b>eui-64</b> ]   <b>autoconfig</b> }	Mandatory  By default, the tunnel interface is not configured with IPv6 address.
	Configure IPv6 link-local addresses.	<b>ipv6 address</b> <i>ipv6-address</i> <b>link-local</b>	Optional  By default, the link-local address is automatically generated when IPv6 is enabled on the interface.
Configure tunnel interface mode as automatically configured IPv4 over IPv6 tunnels.	<b>tunnel mode ipv6ip isatap</b>	Mandatory  By default, the tunnel interface mode is GRE over IPv4.	
Configure the tunnel interface source address or interface name.	<b>tunnel source</b> { <i>ip-address</i>   <i>interface-name</i> }	Mandatory  By default, the tunnel interface is not configured with source address and interface name.	
Configure the tunnel interface to reference the reflection group.	<b>tunnel service-loop</b> <i>service-loop-id</i>	Mandatory  By default, the tunnel interface does not	

Step	Command	Description
		reference the reflection group.

---

### Note

- The ISATAP tunnel does not need to be configured with a destination break address; the destination address used for tunnel encapsulation is automatically obtained from the IPv4 address embedded in the IPv6 address of the ISATAP tunnel.
  - When configuring the tunnel source, if the interface method is used, the primary address of the source interface is taken as the source address of the tunnel.
  - Both ends of the tunnel should be configured to the same tunnel mode, otherwise transmission through the tunnel will fail.
  - Multiple ISATAP tunnels with identical source addresses cannot be configured at the same time on the same device.
- 

#### 47.2.4 Transition Tunnel Monitoring and Maintaining

Refer to GRE Monitoring and Maintenance in Section 7.2.2 of the GRE Configuration Manual.

### 47.3 Typical Configuration Example of Transition Tunnel

#### 47.3.1 Configure basic functions of manually configured IPv6 over IPv4 tunnels.

##### Network Requirements

- IPv6 Network1 and IPv6 Network2 are the private IPv6 networks of Device1 and Device3 respectively.
- IPv6 Network1 and IPv6 Network2 communicate through a IPv6 over IPv4 tunnel between Device1 and Device3.

##### Network Topology

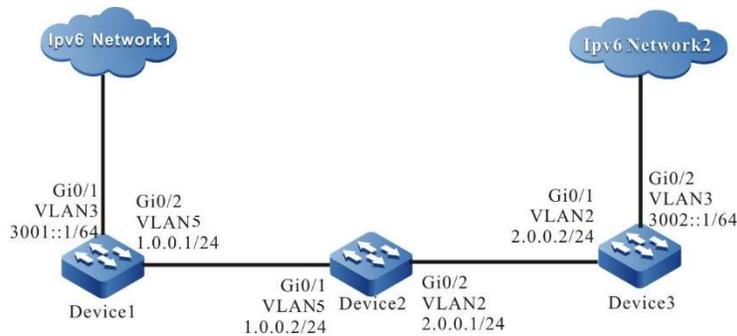


Figure 47-1 Network Topology for Configuring Basic Functions of Manually Configured IPv6 over IPv4 Tunnels

### Configuration Steps

Step 1: Configure IP addresses for the ports. (Omitted)

Step 2: Configure OSPF to enable communication between Device1, Device2, and Device3.

#### #Configure Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#network 1.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#exit
```

#### #Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 1.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#exit
```

#### #Configure Device3.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#exit
```

#### #Check the routing table of Device3.

```
Device3#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

O 1.0.0.0/24 [110/65536] via 2.0.0.1, 00:18:40, vlan2
C 2.0.0.0/24 is directly connected, 00:22:27, vlan2
```

---

 **Note**

- Device1 and Device2 are checked in the same way as Device3, the process of which is omitted.
- 

Step 3: Manually configure IPv6 over IPv4 tunnels.

#Manually configure IPv6 over IPv4 tunnel1 on Device1 with the source address 1.0.0.1, destination address 2.0.0.2, and IPv6 address 10::1.

```
Device1(config)#interface tunnel 1
Device1(config-if-tunnel1)#tunnel mode ipv6ip
Device1(config-if-tunnel1)#tunnel source 1.0.0.1
Device1(config-if-tunnel1)#tunnel destination 2.0.0.2
Device1(config-if-tunnel1)#ipv6 address 10::1/64
Device1(config-if-tunnel1)#exit
```

#Manually configure IPv6 over IPv4 tunnel1 on Device3 with the source address 2.0.0.2, destination address 1.0.0.1, and IPv6 address 10::2.

```
Device3(config)#interface tunnel 1
Device3(config-if-tunnel1)#tunnel mode ipv6ip
Device3(config-if-tunnel1)#tunnel source 2.0.0.2
Device3(config-if-tunnel1)#tunnel destination 1.0.0.1
Device3(config-if-tunnel1)#ipv6 address 10::2/64
Device3(config-if-tunnel1)#exit
```

#Check information about the manually configured IPv6 over IPv4 tunnels of Device3.

```
Device3#show tunnel 1

Tunnel 1:
  Tunnel mode is ipv6ip
  Source ipv4 address is 2.0.0.2 (Source ipv4 address is up on source interface vlan2)
  Destination ipv4 address is 1.0.0.1
  Tunnel state is up
  Encapsulation vrf is global(0x0)
  TTL(time-to-live) is 255
  TOS(type of service) is not set
total(1)
```

---

 **Note**

- Device1 is checked in the same way as that of Device3, the process of which is omitted.
  - When the tunnels are not in the same network segment, you need to configure static routes on the devices at both ends of a local tunnel to reach a peer tunnel, and the output interface is configured as the interface of the local tunnel.
-

Step 4: Configure static routes.

#On Device1, configure a static route to the IPv6 Network2 with the output interface as tunnel1.

```
Device1(config)#ipv6 route 3002::/64 tunnel1
```

#On Device3, configure a static route to the IPv6 Network1 with the output interface as tunnel1.

```
Device3(config)#ipv6 route 3001::/64 tunnel1
```

# Check the IPv6 routing table of Device3.

```
Device3#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
  via ::, 1w6d:20:35:50, lo0
C 10::/64 [0/0]
  via ::, 00:03:31, tunnel1
L 10::2/128 [0/0]
  via ::, 00:03:29, lo0
S 3001::/64 [1/100000]
  via ::, 00:00:01, tunnel1
C 3002::/64 [0/0]
  via ::, 00:00:06, vlan3
L 3002::1/128 [0/0]
  via ::, 00:00:04, lo0
```

---

### Note

- Device1 is checked in the same way as that of Device3, the process of which is omitted.
- 

## 47.3.2 Configure Basic Functions of 6to4 Tunnels

### Network Requirements

- IPv6 Network1 and IPv6 Network2 are the private IPv6 networks of Device1 and Device3 respectively.
- PC1 in IPv6 Network1 and PC2 in IPv6 Network2 communicate through a 6to4 tunnel between Device1 and Device3.

### Network Topology

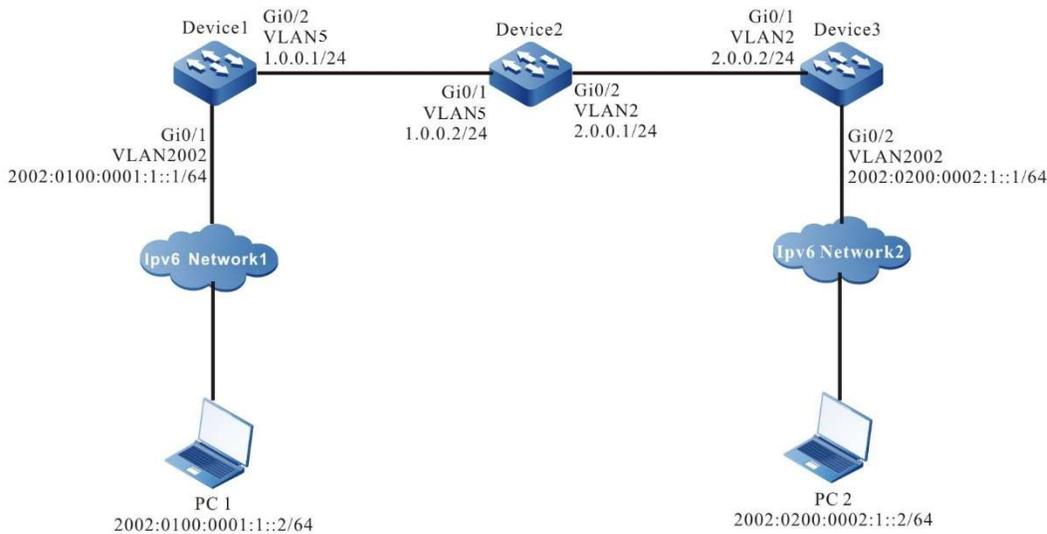


Figure 47-2 Network Topology for Configuring Basic Functions of 6to4 Tunnels

### Configuration Steps

Step 1: Configure IP addresses for the ports. (Omitted)

Step 2: Configure OSPF to enable communication between Device1, Device2, and Device3.

#### #Configure Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#network 1.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#exit
```

#### #Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 1.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#exit
```

#### #Configure Device3.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#exit
```

#### #Check the routing table of Device3.

```
Device3#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

O 1.0.0.0/24 [110/65536] via 2.0.0.1, 00:18:40, vlan2
```

C 2.0.0.0/24 is directly connected, 00:22:27, vlan2

---

## Note

- Device1 and Device2 are checked in the same way as Device3, the process of which is omitted.
- 

Step 3: Create a reflection group, and reference the reflection group on a down port of the device.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#serviceloop-group 1
Device1(config)#inter g0/1
Device1(config-if-gigabitethernet0/1)#serviceloop-group 1 active
This command will clear all config in the interface, Please make sure the interface in default state. Do you want to proceed?
(yes|no)?yes
Device1(config-if-gigabitethernet0/1)#exit
```

#Configure Device3.

```
Device3#configure terminal
Device3(config)#serviceloop-group 1
Device3(config)#inter g0/1
Device3(config-if-gigabitethernet0/1)#serviceloop-group 1 active
This command will clear all config in the interface, Please make sure the interface in default state. Do you want to proceed?
(yes|no)?yes
Device3(config-if-gigabitethernet0/1)#exit
```

Step 4: Configure 6to4 tunnels.

#Configure 6to4 tunnel1 on Device1 with the source address 1.0.0.1, and the tunnel interface referencing a reflection group with the IPv6 address 2002:100:1::1.

```
Device1(config)#interface tunnel 1
Device1(config-if-tunnel1)#tunnel mode ipv6ip 6to4
Device1(config-if-tunnel1)#tunnel source 1.0.0.1
Device1(config-if-tunnel1)#tunnel service-loop 1
Device1(config-if-tunnel1)#ipv6 address 2002:100:1::1/64
Device1(config-if-tunnel1)#exit
```

#Configure 6to4 tunnel1 on Device3 with the source address 2.0.0.2, and the tunnel interface referencing a reflection group with the IPv6 address 2002:200:2::1.

```
Device3(config)#interface tunnel 1
Device3(config-if-tunnel1)#tunnel mode ipv6ip 6to4
Device3(config-if-tunnel1)#tunnel source 2.0.0.2
Device3(config-if-tunnel1)#tunnel service-loop 1
Device3(config-if-tunnel1)#ipv6 address 2002:200:2::1/64
Device3(config-if-tunnel1)#exit
```

#Check information about the 6to4 tunnel on Device3.

```
Device3# show tunnel 1
```

```
Tunnel 1:
```

```
Tunnel mode is ipv6ip 6to4
```

```
Source ipv4 address is 2.0.0.2(Source ipv4 address is up on source interface vlan2)
```

```
Tunnel state is up
```

```
Encapsulation vrf is global(0x0)
```

```
TTL(time-to-live) is 255
```

```
TOS(type of service) is not set
```

```
total(1)
```

---

## Note

- Device1 is checked in the same way as that of Device3, the process of which is omitted.
  - When the tunnels are not in the same network segment, you need to configure static routes on the devices at both ends of a local tunnel to reach a peer tunnel, and the output interface is configured as the interface of the local tunnel.
- 

Step 5: Configure static routes.

#On Device1, configure a static route to the network segment 2002::/16 with the output interface as tunnel1.

```
Device1(config)#ipv6 route 2002::/16 tunnel1
```

#On Device3, configure a static route to the network segment 2002::/16 with the output interface as tunnel1.

```
Device3(config)#ipv6 route 2002::/16 tunnel1
```

# Check the IPv6 routing table of Device3.

```
Device3#show ipv6 route
```

```
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
```

```
U - Per-user Static route
```

```
O - OSPF, OE-OSPF External, M - Management
```

```
L ::1/128 [0/0]
```

```
via ::, 6w1d:02:11:13, lo0
```

```
S 2002::/16 [1/100000]
```

```
via ::, 00:10:31, tunnel1
```

```
C 2002:200:2::/64 [0/0]
```

```
via ::, 00:12:51, tunnel1
```

```
L 2002:200:2::1/128 [0/0]
```

```
via ::, 00:12:49, lo0
```

```
C 2002:200:2:1::/64 [0/0]
```

```
via ::, 00:12:15, vlan2002
```

```
L 2002:200:2:1::1/128 [0/0]
```

```
via ::, 00:12:13, lo0
```

---

 **Note**

- Device1 is checked in the same way as that of Device3, the process of which is omitted.
- 

Step 6: Check the result.

#PC1 pings PC2 at address 2002:200:2:1::2.

```
C:\>ping6 2002:200:2:1::2 -s 2002:0100:0001:1::2

Pinging 2002:200:2:1::2 with 32 bytes of data:

Reply from 2002:200:2:1::2: time<1ms
Reply from 2002:200:2:1::2: time<1ms
Reply from 2002:200:2:1::2: time<1ms
Reply from 2002:200:2:1::2: time<1ms

Ping statistics for 2002:200:2:1::2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

#PC1 is able to ping through to PC2 at address 2002:200:2:1::2.

### 47.3.3 Configure Basic Functions of ISATAP Tunnels

#### Network Requirements

- Device and PC2 can communicate with each other over IPv4 network.
- PC2 acts as the ISATAP host and establishes an ISATAP tunnel with the Device.
- PC1 in the IPv6 Network and PC2 in the IP Network engage in IPv6 communication with each other over the ISATAP tunnel.

#### Network Topology

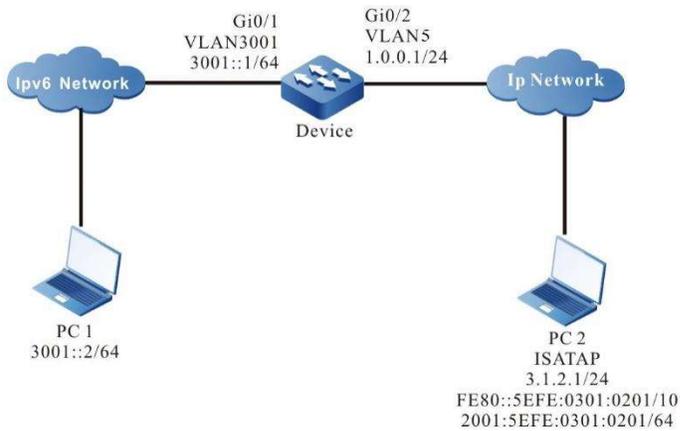


Figure 47-3 Network Topology for Configuring Basic Functions of ISATAP Tunnels

### Configuration Steps

Step 1: Configure IP addresses for the ports. (Omitted)

Step 2: Create a reflection group, and reference the reflection group on a down port of the device.

```
Device#configure terminal
Device(config)#serviceloop-group 1
Device(config)#inter g0/1
Device(config-if-gigabitethernet0/1)#serviceloop-group 1 active
This command will clear all config in the interface, Please make sure the interface in default state. Do you want to proceed?
(yes/no)?yes
Device(config-if-gigabitethernet0/1)#exit
```

Step 3: Configure ISATAP tunnels on Device.

#Configure ISATAP tunnel1 on Device with the source address 1.0.0.1, and the tunnel interface referencing a reflection group with the IPv6 address 2001::5efe:100:1.

```
Device#configure terminal
Device(config)#interface tunnel 1
Device(config-if-tunnel1)#tunnel mode ipv6ip isatap
Device(config-if-tunnel1)#tunnel source 1.0.0.1
Device(config-if-tunnel1)#tunnel service-loop 1
Device(config-if-tunnel1)#ipv6 address 2001::5efe:100:1/64
Device(config-if-tunnel1)#exit
```

#Check the IPv6 routing table of Device.

```
Device#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
U - Per-user Static route
O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
via ::, 6d:05:16:46, lo0
C 2001::/64 [0/0]
via ::, 00:07:56, tunnel1
L 2001::5efe:100:1/128 [0/0]
via ::, 00:07:54, lo0
```

```
C 3001::/64 [0/0]
  via ::, 02:42:37, vlan3001
L 3001::1/128 [0/0]
  via ::, 02:42:36, lo0
```

#Check information about the ISATAP tunnel on Device.

```
Device#show tunnel 1

Tunnel 1:
  Tunnel mode is ipv6ip isatap
  Source ipv4 address is 1.0.0.1(Source ipv4 address is up on source interface vlan5)
  Tunnel state is up
  Encapsulation vrf is global(0x0)
  TTL(time-to-live) is 255
  TOS(type of service) is not set
total(1)
```

Step 4: Disable the RA response suppression function of tunnel1 on Device.

#Disable the RA response suppression function of tunnel1 on Device.

```
Device(config)#interface tunnel 1
Device(config-if-tunnel1)#no ipv6 nd suppress-ra response
Device(config-if-tunnel1)#exit
```

Step 5: Configure ISATAP host PC2.

#The configuration of ISATAP tunnels on hosts varies by operating system, and the Windows XP is used here as an example. #IPv6 protocol is installed on the PC2.

```
C:\>ipv6 install
```

#Normally, when Windows XP installs the IPv6 protocol successfully, the IPv6 interface 2 is taken as the ISATAP interface. Check the information about IPv6 interface 2 on PC2.

```
C:\>ipv6 if 2

Interface 2: Automatic Tunneling Pseudo-Interface

Guid {48FCE3FC-EC30-E50E-F1A7-71172AEEE3AE}

does not use Neighbor Discovery

does not use Router Discovery

routing preference 1

EUI-64 embedded IPv4 address: 0.0.0.0

router link-layer address: 0.0.0.0

  preferred link-local fe80::5efe:3.1.2.1, life infinite

link MTU 1280 (true link MTU 65515)

current hop limit 128

reachable time 42500ms (base 30000ms)
```

```
retransmission interval 1000ms
DAD transmits 0
default site prefix length 48
```

The IPv6 interface 2 of PC2 automatically generates the link-local address fe80::5efe:3.1.2.1 in ISATAP format without obtaining the address prefix.

#Configure the destination address of the ISATAP tunnel as 1.0.0.1 on IPv6 interface 2 of PC2.

```
C:\>ipv6 rlu 2 1.0.0.1
```

#Check information about IPv6 interface 2 on PC2.

```
C:\>ipv6 if 2
Interface 2: Automatic Tunneling Pseudo-Interface
Guid {48FCE3FC-EC30-E50E-F1A7-71172AEEE3AE}
does not use Neighbor Discovery
uses Router Discovery
routing preference 1
EUI-64 embedded IPv4 address: 3.1.2.1
router link-layer address: 1.0.0.1
preferred global 2001::5efe:3.1.2.1, life 29d23h59m46s/6d23h59m46s (public)
preferred link-local fe80::5efe:3.1.2.1, life infinite
link MTU 1500 (true link MTU 65515)
current hop limit 255
reachable time 42500ms (base 30000ms)
retransmission interval 1000ms
DAD transmits 0
default site prefix length 48
```

The ipv6 interface 2 of PC2 obtains the address prefix 2001::/64 and generates the global unicast address 2001::5efe:3.1.2.1.

Step 6: Check the result.

#Ping the IPv6 interface 2 of PC2 on PC1 at address 2001::5efe:3.1.2.1.

```
C:\>ping 2001::5efe:3.1.2.1
Pinging 2001::5efe:3.1.2.1 with 32 bytes of data:
Reply from 2001::5efe:3.1.2.1: time<1ms
Reply from 2001::5efe:3.1.2.1: time<1ms
Reply from 2001::5efe:3.1.2.1 :time<1ms
```

```
Reply from 2001::5efe:3.1.2.1: time<1ms

Ping statistics for 2001::5efe:3.1.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

#PC1 is able to ping through to the IPv6 interface 2 of PC2 at address 2001::5efe:3.1.2.1.

# 48 IPv6 Tunnel

---

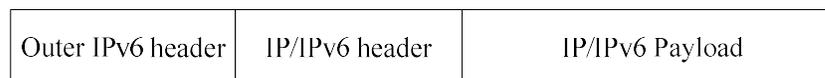
## 48.1 Overview

IPv6 (IPv4 over IPv6/IPv6 over IPv6) tunneling, one of many tunneling technologies, is similar to GRE (Generic Routing Encapsulation) tunneling in that the start and end points of the tunnel need to be manually configured. It is a virtual point-to-point connection that provides a transmission channel for encapsulated packets, with encapsulation and decapsulation of data packets at each end of the tunnel. IPv6 tunnels, which encapsulate both IPv4 data packets and IPv6 packets, enable these encapsulated data packets to be transmitted in IPv6 networks. When the data packet is an IPv4 packet, it is called an IPv4 over IPv6 tunnel, and when the data packet is an IPv6 packet, it is called an IPv6 over IPv6 tunnel, or if it does not distinguish whether the data packet is an IPv4 packet or an IPv6 packet, it is called an IPv6 tunnel.

- IPv4 Over IPv6/IPv6 Over IPv6 Tunnel Encapsulation

When an IPv6/IPv4 data packet is to be sent through an IPv6 tunnel, the tunnel adds an IPv6 packet header with the protocol number set to 4 in the IPv6 packet header, the source address in the IPv6 packet header is set to the source address of the tunnel, and the destination address in the IPv6 packet header is set to the destination address of the tunnel.

- IPv4 Over IPv6/IPv6 Over IPv6 Packet Structure



IP/IPv6 Payload: The IP/IPv6 packet load before entering the tunnel, acting as the payload of the tunnel packet.

IP/IPv6 Header: The header of the IP/IPv6 packet before entering the tunnel.

Outer IPv6 header: The encapsulated external IP packet header, which is a transport tool to enable IP/IPv6 packets to traverse another IPv6 network.

- IPv4 Over IPv6/IPv6 Over IPv6 Packet Forwarding

After the packet is encapsulated at the start of the IPv4 over IPv6/IPv6 over IPv6 tunnel, it is routed according to the encapsulated destination address and then sent out from the corresponding network interface. The intermediate device forwards it as a regular IPv6 packet until it reaches the end of the tunnel.

- IPv4 Over IPv6/IPv6 Over IPv6 Tunnel Decapsulation

The decapsulation process is the opposite of the encapsulation process. The tunnel endpoint receives the packet and analyzes the outer IP header first. If the destination address is its own address, the protocol field in the IPv6 header will be checked, and if the protocol field is 41, the packet is handed over to the IPv4 over IPv6/IPv6 over IPv6 tunnel for processing. After the tunnel removes the Outer IPv6 header of the packet, it performs routing based on the destination address of the decapsulated packet and performs subsequent processing based on the routing result.

## 48.2 IPv6 Tunnel Function Configuration

Table 48-1 IPv6 Tunnel Function Configuration List

Configuration Task	
Configure IPv6 tunnels.	Configure IPv4 over IPv6 tunnels.
	Configure IPv6 over IPv6 tunnels.

### 48.2.1 Configure IPv4 over IPv6 tunnels.

#### Configuration Condition

Before configuring IPv4 over IPv6 tunnels, ensure that

- Configuring the interface IPv4 address to make it reachable at the network layer of adjacent nodes.
- Create the tunnel interface and configure the basic parameters (refer to the tunnel interface configuration manual).
- Configure any unicast routing protocol or static route to make both ends of the tunnel reachable via route.

#### Configure IPv4 Over IPv6 Tunnels

Table 48-1 Configuring IPv4 Over IPv6 Tunnels

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the tunnel interface configuration mode.	interface tunnel tunnel-number	-
Configure tunnel interface addresses.	ip address ip-address { mask   mask-length }	Mandatory  By default, the tunnel interface address is not configured.
Configure the tunnel interface mode as IPv4 over IPv6.	tunnel mode ipipv6	Optional  By default, the tunnel interface mode is GRE over IPv4.
Configure the tunnel interface source address or interface name.	tunnel source { ipv6-address   interface-name }	Mandatory  By default, the tunnel interface is not configured with source address and interface name.
Configure the destination address of the tunnel interface.	tunnel destination { ipv6-address }	Mandatory  By default, the tunnel interface is not configured with destination address.

---

 **Note**

- The tunnel interface address needs to be configured with an IPv4 address, and the passenger protocol can only be an IPv4 protocol.
  - The source and destination addresses must be configured on both ends of the tunnel, and the addresses on both ends must be the source and destination addresses of each other.
-

- 
- When configuring the tunnel source, if the interface method is used, the first IPv6 address of the source interface is taken as the source address of the tunnel (not the linklocal address).
  - Both ends of the tunnel should be configured to the same tunnel mode, otherwise transmission through the tunnel will fail.
- 

## 48.2.2 Configure IPv6 over IPv6 tunnels.

### Configuration Condition

Before configuring IPv6 over IPv6 tunnels, ensure that

- Configuring the interface IPv6 address to make it reachable at the network layer of adjacent nodes.
- Create the tunnel interface and configure the basic parameters (refer to the tunnel interface configuration manual).
- Configure any unicast routing protocol or static route to make both ends of the tunnel reachable via route.

### Configure IPv6 Over IPv6 Tunnels

Table 48-2 Configuring IPv6 Over IPv6 Tunnels

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the tunnel interface configuration mode.	interface tunnel tunnel-number	-
Configure tunnel interface addresses.	ipv6 address ipv6-address { mask   mask-length }	Mandatory By default, no address is configured on the tunnel interface.
Configure the tunnel interface mode as IPv6 over IPv6.	tunnel mode ipv6ipv6	Optional By default, the tunnel interface mode is GRE over IPv4.

Step	Command	Description
Configure the tunnel interface source address or interface name.	tunnel source { ipv6-address   interface-name }	Mandatory By default, the tunnel interface is not configured with source address and interface name.
Configure the destination address or host name of the tunnel interface.	tunnel destination { ipv6-address }	Mandatory By default, the tunnel interface is not configured with destination address.

---

### Note

- The tunnel interface address needs to be configured with an IPv6 address, and the passenger protocol can only be an IPv6 protocol.
  - The source and destination addresses must be configured on both ends of the tunnel, and the addresses on both ends must be the source and destination addresses of each other.
  - When configuring the tunnel source, if the interface method is used, the first IPv6 address of the source interface is taken as the source address of the tunnel (not the linklocal address).
  - Both ends of the tunnel should be configured to the same tunnel mode, otherwise transmission through the tunnel will fail.
- 

### 48.2.3 IPv6 Tunnel Monitoring and Maintaining

Refer to GRE Monitoring and Maintenance in Section 7.2.2 of the GRE Configuration Manual.

## 48.3 Typical Configuration Example of IPv6 Tunnel

### 48.3.1 Configure Basic Functions of IPv4 Over IPv6

#### Network Requirements

- IP Network1 and IP Network2 are the private IP networks of Device1 and Device3 respectively.
- IP Network1 and IP Network2 communicate through a IPv6 tunnel between Device1

and Device3.

## Network Topology

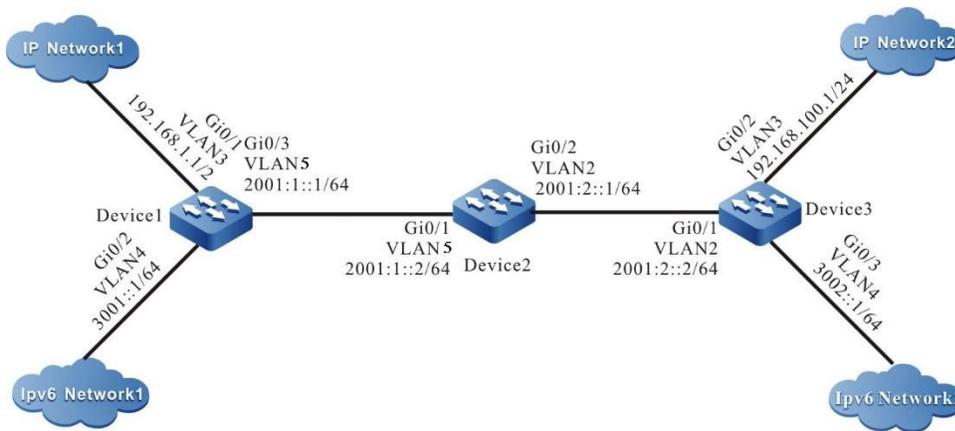


Figure 48-2 Network Topology for Configuring Basic Functions of IPv6 Tunnels

## Configuration Steps

Step 1: Configure IP addresses for the ports. (Omitted)

Step 2: Configure OSPFv3 to enable communication between Device1, Device2, and Device3.

### #Configure Device1.

```
Device1#configure terminal
Device1(config)#ipv6 router ospf 100
Device1(config-ospf6)#router-id 1.1.75.1
Device1(config-ospf6)#exit
Device1(config)#interface vlan5
Device1(config-if-vlan5)#ipv6 router ospf tag 100 area 0
Device1(config-if-vlan5)#exit
```

### #Configure Device2.

```
Device2#configure terminal
Device2(config)#ipv6 router ospf 100
Device2(config-ospf6)#router-id 1.2.75.1
Device2(config-ospf6)#exit
Device2(config)#interface vlan5
Device2(config-if-vlan5)#ipv6 router ospf tag 100 area 0
Device2(config-if-vlan5)#exit
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ipv6 router ospf tag 100 area 0
Device2(config-if-vlan2)#exit
```

### #Configure Device3.

```
Device3#configure terminal
Device3(config)#ipv6 router ospf 100
Device3(config-ospf6)#router-id 1.1.73.1
Device3(config-ospf6)#exit
Device3(config)#interface vlan2
Device3(config-if-vlan2)#ipv6 router ospf tag 100 area 0
```

```
Device3(config-if-vlan2)#exit
```

### # Check the IPv6 routing table of Device3.

```
Device3#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management
```

```
L ::1/128 [0/0]
   via ::, 6w0d:23:09:31, lo0
O 2001:1::/64 [110/2]
   via fe80::508b:fff:fee4:ff6, 00:08:37, vlan2
C 2001:2::/64 [0/0]
   via ::, 00:15:51, vlan2
L 2001:2::2/128 [0/0]
   via ::, 00:15:50, lo0
C 3002::/64 [0/0]
   via ::, 00:15:06, vlan4
L 3002::1/128 [0/0]
   via ::, 00:15:04, lo0
```

---

## Note

- Device1 and Device2 are checked in the same way as Device3, the process of which is omitted.
- 

### Step 3: Configure IPv6 tunnels.

#Configure IPv6 tunnel1 on Device1, with the source address 2001:1::1, destination address 2001:2::2, IP address 10.0.0.1, and IPv6 address 10::1.

```
Device1(config)#interface tunnel 1
Device1(config-if-tunnel1)#tunnel mode ipipv6
Device1(config-if-tunnel1)#tunnel source 2001:1::1
Device1(config-if-tunnel1)#tunnel destination 2001:2::2
Device1(config-if-tunnel1)#ip address 10.0.0.1 255.255.255.0
Device1(config-if-tunnel1)#ipv6 address 10::1/64
Device1(config-if-tunnel1)#exit
```

#Configure IPv6 tunnel1 on Device3, with the source address 2001:2::2, destination address 2001:1::1, IP address 10.0.0.2, and IPv6 address 10::2.

```
Device3(config)#interface tunnel 1
Device3(config-if-tunnel1)#tunnel mode ipipv6
Device3(config-if-tunnel1)#tunnel source 2001:2::2
Device3(config-if-tunnel1)#tunnel destination 2001:1::1
Device3(config-if-tunnel1)#ip address 10.0.0.2 255.255.255.0
Device3(config-if-tunnel1)#ipv6 address 10::2/64
Device3(config-if-tunnel1)#exit
```

#Check information about IPv6 tunnel of Device3.

```
Device3#show tunnel 1
```

```
Tunnel 1:
```

```
Tunnel mode is ipipv6  
Source ipv6 address is 2001:2::2(Source ipv6 address is up on source interface vlan2)  
Destination ipv6 address is 2001:1::1  
Tunnel state is up  
Encapsulation vrf is global(0x0)  
TTL(time-to-live) is 255  
TOS(type of service) is not set
```

```
total(1)
```

---

## Note

- Device1 is checked in the same way as that of Device3, the process of which is omitted.
  - When the tunnels are not in the same network segment, you need to configure static routes on the devices at both ends of a local tunnel to reach a peer tunnel, and the output interface is configured as the interface of the local tunnel.
- 

Step 4: Configure static routes.

#On Device1, configure a static route to the IP Network2 with the output interface as tunnel1.

```
Device1(config)#ip route 192.168.100.0 255.255.255.0 tunnel1
```

#On Device3, configure a static route to the IP Network1 with the output interface as tunnel1.

```
Device3(config)#ip route 192.168.1.0 255.255.255.0 tunnel1
```

#Check the routing table of Device3.

```
Device3#show ip route  
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management  
D - Redirect, E - IRMP, EX - IRMP external, o - SNRP, B - BGP, i-ISIS
```

```
Gateway of last resort is not set
```

```
C 10.0.0.0/24 is directly connected, 00:17:12, tunnel1  
S 192.168.1.0/24 [1/100000] is directly connected, 00:00:10, tunnel1  
C 192.168.100.0/24 is directly connected, 00:00:28, vlan3
```

---

## Note

- Device1 is checked in the same way as that of Device3, the process of which is omitted.
-

## 48.3.2 Configure Basic Functions of IPv6 Over IPv6

### Network Requirements

- IPv6 Network1 and IPv6 Network2 are the private IPv6 networks of Device1 and Device3 respectively.
- IPv6 Network1 and IPv6 Network2 communicate through a IPv6 tunnel between Device1 and Device3.

### Network Topology

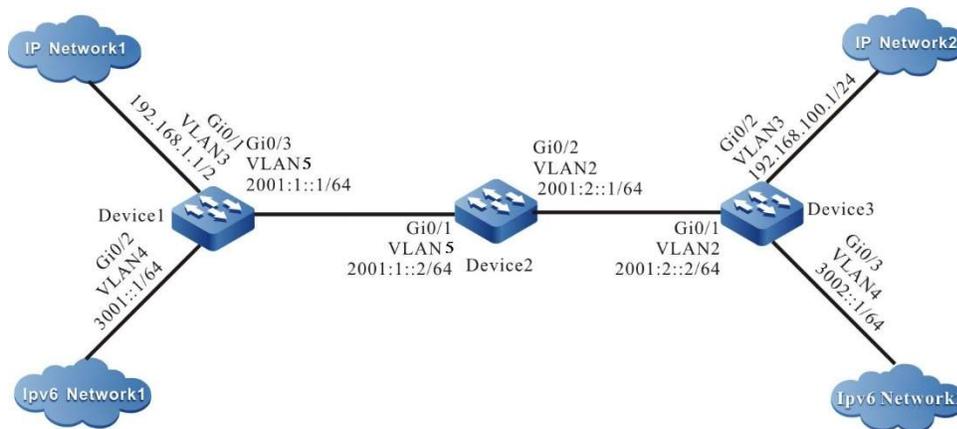


Figure 48-3 Network Topology for Configuring Basic Functions of IPv6 Tunnels

### Configuration Steps

Step 1: Configure IP addresses for the ports. (Omitted)

Step 2: Configure OSPFv3 to enable communication between Device1, Device2, and Device3.

#### #Configure Device1.

```
Device1#configure terminal
Device1(config)#ipv6 router ospf 100
Device1(config-ospf6)#router-id 1.1.75.1
Device1(config-ospf6)#exit
Device1(config)#interface vlan5
Device1(config-if-vlan5)#ipv6 router ospf tag 100 area 0
Device1(config-if-vlan5)#exit
```

#### #Configure Device2.

```
Device2#configure terminal
Device2(config)#ipv6 router ospf 100
Device2(config-ospf6)#router-id 1.2.75.1
Device2(config-ospf6)#exit
Device2(config)#interface vlan5
```

```
Device2(config-if-vlan5)#ipv6 router ospf tag 100 area 0
Device2(config-if-vlan5)#exit
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ipv6 router ospf tag 100 area 0
Device2(config-if-vlan2)#exit
```

### #Configure Device3.

```
Device3#configure terminal
Device3(config)#ipv6 router ospf 100
Device3(config-ospf6)#router-id 1.1.73.1
Device3(config-ospf6)#exit
Device3(config)#interface vlan2
Device3(config-if-vlan2)#ipv6 router ospf tag 100 area 0
Device3(config-if-vlan2)#exit
```

### # Check the IPv6 routing table of Device3.

```
Device3#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
   via ::, 6w0d:23:09:31, lo0
O 2001:1::/64 [110/2]
   via fe80::508b:fff:fee4:ff6, 00:08:37, vlan2
C 2001:2::/64 [0/0]
   via ::, 00:15:51, vlan2
L 2001:2::2/128 [0/0]
   via ::, 00:15:50, lo0
C 3002::/64 [0/0]
   via ::, 00:15:06, vlan4
L 3002::1/128 [0/0]
   via ::, 00:15:04, lo0
```

---

## Note

- Device1 and Device2 are checked in the same way as Device3, the process of which is omitted.
- 

### Step 3: Configure IPv6 tunnels.

#Configure IPv6 tunnel1 on Device1, with the source address 2001:1::1, destination address 2001:2::2, IP address 10.0.0.1, and IPv6 address 10::1.

```
Device1(config)#interface tunnel 1
Device1(config-if-tunnel1)#tunnel mode ipv6ip6
Device1(config-if-tunnel1)#tunnel source 2001:1::1
Device1(config-if-tunnel1)#tunnel destination 2001:2::2
Device1(config-if-tunnel1)#ip address 10.0.0.1 255.255.255.0
Device1(config-if-tunnel1)#ipv6 address 10::1/64
Device1(config-if-tunnel1)#exit
```

#Configure IPv6 tunnel1 on Device3, with the source address 2001:2::2, destination address 2001:1::1, IP address 10.0.0.2, and IPv6 address 10::2.

```
Device3(config)#interface tunnel 1
Device3(config-if-tunnel1)#tunnel mode ipv6ipv6
Device3(config-if-tunnel1)#tunnel source 2001:2::2
Device3(config-if-tunnel1)#tunnel destination 2001:1::1
Device3(config-if-tunnel1)#ip address 10.0.0.2 255.255.255.0
Device3(config-if-tunnel1)#ipv6 address 10::2/64
Device3(config-if-tunnel1)#exit
```

#Check information about IPv6 tunnel of Device3.

```
Device3#show tunnel 1

Tunnel 1:
  Tunnel mode is ipv6ipv6
  Source ipv6 address is 2001:2::2(Source ipv6 address is up on source interface vlan2)
  Destination ipv6 address is 2001:1::1
  Tunnel state is up
  Encapsulation vrf is global(0x0)
  TTL(time-to-live) is 255
  TOS(type of service) is not set

total(1)
```

---

## Note

- Device1 is checked in the same way as that of Device3, the process of which is omitted.
  - When the tunnels are not in the same network segment, you need to configure static routes on the devices at both ends of a local tunnel to reach a peer tunnel, and the output interface is configured as the interface of the local tunnel.
- 

Step 4: Configure static routes.

#On Device1, configure a static route to the IPv6 Network2 with the output interface as tunnel1.

```
Device1(config)#ipv6 route 3002::/64 tunnel1
```

#On Device3, configure a static route to the IPv6 Network1 with the output interface as tunnel1.

```
Device3(config)# ipv6 route 3001::/64 tunnel1
```

# Check the IPv6 routing table of Device3.

```
Device3#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L  ::1/128 [0/0]
   via ::, 6w0d:23:50:28, lo0
```

```
C 10::/64 [0/0]
  via ::, 00:12:23, tunnel1
L 10::2/128 [0/0]
  via ::, 00:12:22, lo0
O 2001:1::/64 [110/2]
  via fe80::508b:fff:fee4:ff6, 00:49:34, vlan2
C 2001:2::/64 [0/0]
  via ::, 00:56:48, vlan2
L 2001:2::2/128 [0/0]
  via ::, 00:56:46, lo0
S 3001::/64 [1/100000]
  via ::, 00:00:14, tunnel1
C 3002::/64 [0/0]
  via ::, 00:56:02, vlan4
L 3002::1/128 [0/0]
  via ::, 00:56:01, lo0
```

---

### Note

- Device1 is checked in the same way as that of Device3, the process of which is omitted.
- 

# 49 Routing Basics

---

## 49.1 Overview

After a device receives a packet through an interface, the device selects a route according to the destination of the route and then forwards the packet to another interface. This process is called routing. In network devices, routes are stored in a routing table database. The packets search the routing table to determine the next hop and output interface according to the destination of the packets. Routes are categorized into three types according to their sources.

- Direct route: The route is generated based on the interface address. After a user configures the IP address of an interface, the device generates a direct route of the

network segment according to the IP address and mask.

- Static route: The route is manually configured by the user.
- Dynamic route: The route is discovered through the dynamic route discovery protocol. Based on whether the dynamic routing protocol is used within an autonomous domain, two types of dynamic routing protocols are available: Interior Gateway Protocol (IGP) and Exterior Gateway Protocol (EGP). Here an autonomous domain refers to a network which has a unified management organization and unified routing policy. A routing protocol that is used within an autonomous domain is an IGP. Common IGPs include Routing Information Protocol (RIP) and Open Shortest Path First (OSPF). EGPs are usually used for routing among multiple autonomous domains. A common EGP is BGP.

Routing supports load balancing, that is, multiple routes to the same destination. In forwarding packets, a device transmits packets in load balancing mode according to the routing table search result.

## 49.2 Routing Basic Function Configuration

Table 49 Routing Basic Function Configuration List

Configuration Task	
Configure load balancing for routing.	Configure the maximum number of load balancing entries.
	Configure the load balancing calculation method
Configure the capacity of routes for Virtual Route Forwarding (VRF) routes.	Configure the capacity of routes for Virtual Route Forwarding (VRF) routes.

### 49.2.1 Configure load balancing for routing.

#### Configuration Condition

None

#### Configure the maximum number of load balancing entries.

If the costs of several paths to one destination are the same, the paths form load balancing. Configuring the maximum number of load balancing entries helps to improve the link utility rate and reduce the load of links.

Table 1 Configuring Maximum Number of Load Balancing Entries

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the maximum number of load balancing entries.	<b>route path-limit</b> <i>max-number</i>	Optional By default, the maximum number of load balancing entries for routing is 4.

### Configure the load balancing calculation method

There are three load balancing calculation methods:

- Based on source and destination address: Identify a flow with source address and a destination address. The packets of the same flow follow the same path to keep in order. When the loads of each flow are not balanced, the unbalancing of line loads may be caused.
- Based on source address: Identify a flow with source address only. The packets of the same flow use the same path so that the same flow follows the same path to keep in order. When the loads of each flow are not balanced, the unbalancing of line loads may be caused.
- Based on packets: The packets going to the same destination follow different paths to achieve load balancing on each path as much as possible. But they may be out of order.

Table 1-3 Configuring Load Balancing Calculation Method

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure IPv4 packet load balancing method	<b>ip load-sharing { per-destination   per-packet   per-source }</b>	Optional By default, the calculation method based on source and address address is used.

## 49.2.2 Configure the capacity of routes for Virtual Route Forwarding (VRF) routes.

### Configuration Condition

None

### Configure the capacity of routes for Virtual Route Forwarding (VRF) routes.

To ensure normal use of devices and prevents a large number of routes from consuming too many resources, you can use the routing-table limit command to limit the capacity of routes for each Virtual Route Forwarding (VRF). When the capacity of routes reaches the threshold, an alarm is generated.

Table 2 Configuring Capacity of VRF Routes

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the VRF configuration mode	<b>ip vrf vrf-name</b>	-
Configure the capacity of routes for Virtual Route Forwarding (VRF) routes.	<b>routing-table limit limit-value { threshold-value   syslog-alert }</b>	Optional By default, the route capacity is 880000. When the number of routes reaches 80% of the capacity, warning information is printed.

---

### Note

- This command cannot limit the route capacity under global VRF.
  - If the routing entries exceed the capacity, the new routing information will be lost.
-

### 49.2.3 Routing Basic Monitoring and Maintaining

Table 3 Routing Basic Monitoring and Maintaining

Command	Description
<b>clear ip route</b> [ <b>vrf</b> <i>vrf-name</i> ] { <i>ip-address</i> <i>mask</i>   <b>all</b> }	Clear the specified IP routes in the routing table
<b>show ip route</b> [ <b>vrf</b> <i>vrf-name</i> ] [ <b>bgp</b>   <b>connected</b>   <b>irmp</b>   <b>isis</b>   <b>ospf</b>   <b>rip</b>   <b>static</b>   <b>statistic</b> [ <b>all</b> ]   <i>ip-address</i> { <i>mask</i>   <i>mask-len</i> } ]	Show the information of IP routes

# 50 IPv6 Routing Basics

---

## 50.1 Overview

After a device receives an IPv6 packet through an interface, the device selects a route according to the destination of the IPv6 packet and then forwards it to another interface. This process is called routing. In network devices, routes are stored in a routing table database. The packets search the routing table to determine the next hop and output interface according to the destination of the packets. Routes are categorized into three types according to their sources.

- Direct route: The route is generated based on the interface address. After a user configures the IPv6 address of an interface, the device generates a direct route of the network segment according to the this address and mask.
- Static route: The route is manually configured by the user.
- Dynamic route: The route is discovered through the dynamic route discovery protocol. Based on whether the dynamic routing protocol is used within an autonomous domain, two types of dynamic routing protocols are available: Interior Gateway Protocol (IGP) and Exterior Gateway Protocol (EGP). Here an autonomous domain refers to a network which has a unified management organization and unified routing policy. A routing protocol that is used within an autonomous domain is an IGP. Common IGPs include RIPng and OSPFv6. Exterior Gateway Protocols (EGPs) are usually used for routing among multiple autonomous domains. A common EGP is IPv6 BGP.

Routing supports load balancing, that is, multiple routes to the same destination. In forwarding packets, a device transmits packets in load balancing mode according to the routing table search result.

## 50.2 IPv6 routing basic function configuration

Table 50 IPv6 Routing Basic Function Configuration List

Configuration Task	
Configure IPv6 routing load balancing	Configure IPv6 load balancing calculation method

## 50.2.1 Configure IPv6 routing load balancing

### Configuration Condition

None

### Configure IPv6 load balancing calculation method

There are three load balancing calculation methods:

- Based on source and destination address: Identify a flow with source address and a destination address. The packets of the same flow follow the same path to keep in order. When the loads of each flow are not balanced, the unbalancing of line loads may be caused.
- Based on source address: Identify a flow with source address only. The packets of the same flow use the same path so that the same flow follows the same path to keep in order. When the loads of each flow are not balanced, the unbalancing of line loads may be caused.
- Based on packets: The packets going to the same destination follow different paths to achieve load balancing on each path as much as possible. But they may be out of order.

Table 50 Configuring IPv6 Load Balancing Calculation Method

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure IPv6 packet load balancing method	<b>ipv6 load-sharing { per-destination   per-packet   per-source }</b>	Optional By default, the calculation method based on source and address address is used.

## 50.2.2 IPv6 routing basic monitoring and maintaining

Table 1 IPv6 Routing Basic Monitoring and Maintaining

Command	Description
<b>clear ipv6 route</b> { <i>ipv6-address</i>   <i>ipv6-prefix</i>   <b>all</b> }	Clear the specified IPv6 routes in the routing table
<b>show ipv6 route</b> [ <b>vrf</b> <i>vrf-name</i> ] [ <i>ipv6-address</i>   <i>ipv6-prefix</i>   <b>bgp</b>   <b>brief</b>   <b>connected</b>   <b>isis</b>   <b>linklocal</b>   <b>local</b>   <b>ospf</b>   <b>rip</b>   <b>static</b>   <b>statistic</b>   <b>all</b> ]	Show the information of IPv6 routes

# 51 Static Routes

---

## 51.1 Overview

A static route is a self-defined route which is manually configured by a user. It specifies a path for transmitting IP packets which are targeted at a specified destination.

Compared with dynamic routing, static routing has higher security and lower device resource occupancy. The disadvantage is that when the network topology changes, manual configuration is required, and there is no automatic re-configuration mechanism.

Static routes do not occupy line bandwidth or occupy CPU to calculate and advertise routes periodically, improving the device and network performance.

Static routes can be used to ensure the security of a small-scale network, for example, in a network where there is only one path connecting to an external network. In a large-scale network, static routes can implement security control on services or links of certain types. A majority of networks adopt dynamic routing protocols but you can still configure some static routes for special purposes.

Static routes can be re-distributed to a dynamic routing protocol, but dynamic routes cannot be re-distributed to static routes. Note that improper static route configuration may cause routing loops.

The default route is a special route which can be a static route. In a routing table, the default route is a route to network 0.0.0.0 with the mask 0.0.0.0. You can use the `show ip route` command to check whether the route is valid. When the destination address of a received packet does not match any entry in the routing table, the packet takes the default route. If no default route is available and the destination is not in the routing table, the packet is discarded, and an ICMP packet is returned to the source end reporting that the destination address or network is not reachable. To prevent the routing table from becoming too large, you can set a default route. The packet that fails to find a matching routing table entry takes the default route for forwarding.

Null0 route is a special route with an Null0 interface. Null0 interface is always UP, though it cannot forward data packets. The data packets sent to this interface are all discarded. When a static route is configured to reach the output interface Null0 of a certain network segment, any packet sent to that network segment will be discarded. Therefore, the packet filtering function can be implemented by configuring a Null0 static route.

## 51.2 Static Routing Function Configuration

Table 51 Static Routing Function Configuration List

Configuration Task	
Configure a Static Route	Configure a Static Route
Configure the Default Administrative Distance	Configure the Default Administrative Distance
Configure the Recursive Function	Configure the Recursive Function
Configure Load Balancing Routes	Configure Load Balancing Routes
Configure a Floating Route	Configure a Floating Route
Configure a Static Route to Coordinate with BFD	Configure a Static Route to Coordinate with BFD
Configure a Static Route to Coordinate with Track	Configure a Static Route to Coordinate with Track

### 51.2.1 Configure a Static Route

#### Configuration Condition

Before configuring a static route, ensure that:

- The link layer protocol has been configured to ensure normal communication at the link layer.
- Interface IP addresses have been configured so that neighbor nodes are reachable at the network layer.

#### Configure a Static Route

According to the parameters that have been specified, static routes are categorized into the following three types:

- Interface route: For an interface route, only the output interface is specified.
- Gateway route: For a gateway route, only the gateway address is specified.
- Interface gateway route: For an interface gateway route, both the output interface and the gateway address are specified.

Configured static routes become invalid if some of the following conditions are met:

- 1) The destination address is the local interface address.
- 2) The destination address is the network of the local direct interface.
- 3) The administrative distance of the route is 255.
- 4) The output interface of the route is DOWN.
- 5) No IP address has been configured for the output interface of the route.
- 6) The gateway address is not reachable.
- 7) The output interface and the gateway of the route conflict.
- 8) The output interface of the route does not exist.
- 9) The TRACK object that is associated with the route is "fake".
- 10) The status of the Bidirectional Forwarding Detection (BFD) session that is associated with the route is DOWN.

If an interface route meets any one condition among 1), 2), 3), 4), 5), 8), and 10), the route is invalid. If a gateway route meets any one condition among 1), 2), 3), 4), 6), 8), 9), and 10), the route is invalid. If an interface gateway route meets any of the above conditions, the route is invalid.

Table 51 Configuring Static Route

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure a Static Route	<b>ip route [ vrf vrf-name1 destination-ip-address destination-mask { interface-name / [ nexthop-ip-address [ vrf vrf-name2 ] ] } [ name nexthop-name ] [ tag tag-value ] [ track track-id ] [ administrative-distance ]</b>	Mandatory  <i>Administrative-distance</i> is the administrative distance of the static route. When it is not specified, the default value is used.

### Note

- When configuring the default route, both destination network and mask should be 0.0.0.0.
- The output interface of Null0 route should be configured as Null0.
- No IP address is required for the output interface of Null0 route.

## 51.2.2 Configure the Default Administrative Distance

### Configuration Condition

None

### Configure the Default Administrative Distance

The smaller the administrative distance that is specified for a static route in configuring the static route is, the higher the priority of the route is. If the administrative distance is not specified, the default administrative distance is used. You can modify the default administrative distance dynamically. After the default administrative distance is re-configured, the new default administrative distance is valid only for new static routes.

Table 1 Configuring Default Administrative Distance

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enters the static route configuration mode.	<b>router static</b>	-
Configure the Default Administrative Distance	<b>distance</b> <i>administration-distance</i>	Optional The value of default administrative distance is 1.

---

### Note

- When using the **ip route** command to configure a static route, you can specify the administrative distance separately (*administrative-distance* parameter). If the administrative distance is not specified, use the default administrative distance.
- 

## 51.2.3 Configure the Recursive Function

### Configuration Condition

None

## Configure the Recursive Function

If the gateway address that is configured for a route is valid only when a route to the gateway is reachable, you must enable the recursive function of the static route to validate the route. By default, the recursive function is enabled for a static route.

Table 2 Configuring Recursive Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enters the static route configuration mode.	<b>router static</b>	-
Configure a static route to support the recursive function.	<b>recursion</b>	Optional By default, a static route supports the recursive function for routing.

## 51.2.4 Configure Load Balancing Routes

### Configuration Condition

None

### Configure Load Balancing Routes

Load balancing routes means that multiple routes are configured to the same destination network. The output interfaces and the gateway addresses of the routes are different, but the administrative distances (priorities) of the routes are the same. Load balancing routes help to improve the link utility rate.

Table 3 Configuring Load Balancing Route

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the first load balancing route	<b>ip route</b> <i>destination-ip-address destination-mask interface-name1 distance</i>	Mandatory The output interface is interface-name1.

Step	Command	Description
Configure the second load balancing route	<b>ip route</b> <i>destination-ip-address destination-mask interface-name2 distance</i>	Mandatory The output interface is <i>interface-name2</i> .

## Note

- When configuring the load balancing route, the *distance* values should be equal.

### 51.2.5 Configure a Floating Route

#### Configuration Condition

None

#### Configure a Floating Route

Multiple routes are available to the same destination network. The output interfaces or gateway addresses of the routes are different, and the priorities of the routes are also different. The route with the higher priority becomes the primary route while the route with the lower priority becomes the floating route. In the routing table, only the primary route is visible. The floating table appears in the routing table only when the primary route becomes invalid. Therefore, the floating route is usually used as a backup route.

Table 4 Configuring Floating Route

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the preferred route	<b>ip route</b> <i>destination-ip-address destination-mask interface-name1 distance1</i>	Mandatory The output interface of preferred route is <i>interface-name1</i> , and the priority is <i>distance1</i> .
Configure a Floating Route	<b>ip route</b> <i>destination-ip-address destination-mask interface-name2 distance2</i>	Mandatory The output interface of the floating route is <i>interface-name2</i> , and the

Step	Command	Description
		priority is <i>distance2</i> . The value of <i>distance2</i> should be greater than <i>distance1</i> .

### Note

- For the priority of the specified route, the smaller the *distance* value, the higher the priority.

## 51.2.6 Configure a Static Route to Coordinate with BFD

### Configuration Condition

None

### Configure a Static Route to Coordinate with BFD

The BFD (Bidirectional Forwarding Detection) protocol can quickly detect the connection status of the forwarding path between two adjacent routers under a light load. By using this method, the protocol neighbor can quickly identify the connection failure of the forwarding path. Unlike other dynamic protocol routing, static routing cannot detect communication link failures. BFD enables static routing to quickly detect these communication link failures. By making static routing coordinate with BFD, you can realize fast switch between routes. Currently, static routing only allows to establish an asynchronous BFD detection mode, so it is necessary to coordinate with BFD on the devices at both ends of the link.

When the BFD status associated with static route is DOWN, the static route configured will become invalid.

Table 51 Configuring Coordination of Static Route with BFD

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure a static route	<b>ip route</b> <i>destination-ip-address destination-mask interface-name nexthop-ip-address</i>	Mandatory Only the static route with the output interface and gateway address specified at the same

Step	Command	Description
		time can coordinate with BFD
Configure the output interface and next hop address of the route associated with BFD	<b>ip route static bfd</b> <i>interface-name nexthop-ip-address</i>	Mandatory <i>nexthop-ip-address</i> is the next hop address of direct route

---

### Note

- For bfd introduction and its basic function configuration, refer to the bfd-related section in the User Manual;
- 

## 51.2.7 Configure a Static Route to Coordinate with Track

### Configuration Condition

None

### Configure a Static Route to Coordinate with Track

Some modules in the system need to monitor some system information and then determine their working modes based on the information. The objects that are monitored by the other modules are called monitoring objects. To simplify the relations between the modules and monitoring objects, Track objects are used. A Track object can contain multiple monitoring objects, and it displays the comprehensive status of the monitoring object to external modules. The external modules are associated only with Track objects and they do not care about monitoring objects contained in the Track objects any more. A Track object has two statuses, "true" and "false". The external modules that are associated with the Track object determine its working modes according to the Track object status.

A static route can associate with a Track object to monitor system information and determine whether the route is valid according to the status reported by the Track object. If the Track object reports "true", the conditions required by the static route are satisfied, and the route is added to the routing table. If the Track object reports "false", the route is deleted from the routing table.

Table 5 Configuring a Static Route to Coordinate with TRACK

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Create Track object and enter its configuration mode	<b>track track-id</b>	Mandatory
Configure the link status of the specified interface for Track object monitoring	<b>interface interface-name line-protocol</b>	Optional
Return to the global configuration mode	<b>exit</b>	-
Configure a static route and associate with Track	<b>ip route destination-ip-address destination-mask interface-name track track-id</b>	Mandatory When the link layer of the monitoring interface is UP, the route takes effect; otherwise, it becomes invalid.

## 51.2.8 Configure static route FRR

### Configuration Condition

Before configuring static route FRR, ensure that:

- Use a routing map to specify the output interface and next hop address of the backup route;

### Configure static route FRR

In the network using static route, the traffic interruption caused by link or device failure will continue until the protocol detects the link failure. It recovers only after the floating route takes effect in several seconds. Static route FRR can reduce the time of traffic interruption. By applying the routing map, set a backup next hop for the successfully matched route. Once the main link fails, the traffic passing through the main link will immediately switch to the backup link, achieving the purpose of fast switching.

Table 51 Configuring Static Route FRR

To...	Command	Description
Enter the system	<b>configure terminal</b>	-

To...	Command	Description
configuration mode		
Configure static route FRR	<b>ip route static fast-reroute route-map</b> <i>map-name</i>	Mandatory By default, the FRR is disabled.
Configure automatic FRR of static route	<b>ip route static pic</b>	Mandatory By default, the automatic FRR is disabled.

---

### Note

- FRR is applicable to the static route with the output interface and gateway address specified at the same time only;
  - When the FRR based on route-map set fast-reroute backup-nexthop is auto, the protocol enables automatic FRR.
  - When pic method is used, the protocol enables automatic FRR.
  - The methods of enabling FRR are mutually exclusive.
- 

## 51.2.9 Static route monitoring and maintaining

Table 6 Static Route Monitoring and Maintaining

Command	Description
<b>show ip route [ vrf vrf-name ] static</b>	Show the static route in the routing table
<b>show running-config ip route</b>	Show the configuration information of static route

## 51.3 Typical configuration example of static route

### 51.3.1 Configure basic functions of static route

#### Network Requirements

- Configure static routes for Device1, Device2 and Device3 to achieve intercommunication between PC1 and PC2.

#### Network Topology



Figure 51 Network Topology for Configuring Basic Functions of Static Route

#### Configuration Steps

Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configures IP addresses for the ports. (Omitted)

Step 3: Configure static routes.

#### #Configure Device1.

```
Device1#configure terminal
Device1(config)#ip route 20.1.1.0 255.255.255.0 10.1.1.2
Device1(config)#ip route 100.1.1.0 255.255.255.0 10.1.1.2
```

#### #Configure Device2.

```
Device2#configure terminal
Device2(config)#ip route 110.1.1.0 255.255.255.0 10.1.1.1
Device2(config)#ip route 100.1.1.0 255.255.255.0 20.1.1.2
```

#### #Configure Device3.

```
Device3#configure terminal
Device3(config)#ip route 0.0.0.0 0.0.0.0 20.1.1.1
```

#### #View the routing table of Device1.

```
Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
U - Per-user Static route
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
C 10.1.1.0/24 is directly connected, 00:06:47, vlan3
S 20.1.1.0/24 [1/100] via 10.1.1.2, 00:00:13, vlan3
S 100.1.1.0/24 [1/100] via 10.1.1.2, 00:00:05, vlan3
C 110.1.1.0/24 is directly connected, 00:08:21, vlan2
C 127.0.0.0/8 is directly connected, 28:48:33, lo0
```

#### #View the routing table of Device 2.

```
Device2#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 10.1.1.0/24 is directly connected, 00:00:37, vlan2
C 20.1.1.0/24 is directly connected, 00:00:27, vlan3
S 100.1.1.0/24 [1/100] via 20.1.1.2, 00:00:05, vlan3
S 110.1.1.0/24 [1/100] via 10.1.1.1, 00:00:13, vlan2
C 127.0.0.0/8 is directly connected, 30:13:18, lo0
```

#### #Check the routing table of Device3.

```
Device3#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

S 0.0.0.0/0 [1/100] via 20.1.1.1, 00:00:07, vlan2
C 20.1.1.0/24 is directly connected, 00:00:08, vlan2
C 100.1.1.0/24 is directly connected, 00:00:13, vlan3
C 127.0.0.0/8 is directly connected, 29:17:19, lo0
```

Step 4: Check the result. Use the **ping** command to check the connectivity between PC1 and PC2.

#### #Use the **ping** command to check connectivity on PC1.

```
C:\Documents and Settings\Administrator>ping 100.1.1.2

Pinging 100.1.1.2 with 32 bytes of data:

Reply from 100.1.1.2: bytes=32 time<1ms TTL=125

Ping statistics for 100.1.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

PC1 and PC2 can communicate with each other.

### 51.3.2 Configure static floating route

#### Network Requirements

- On Device1, configure two static routes leading to the network segment 192.168.1.0/24, one through Device2 and the other through Device3.
- Device1 prefers to use the line between it and Device2 to forward packets; when this line fails, it will switch to Device3 for communication.

## Network Topology

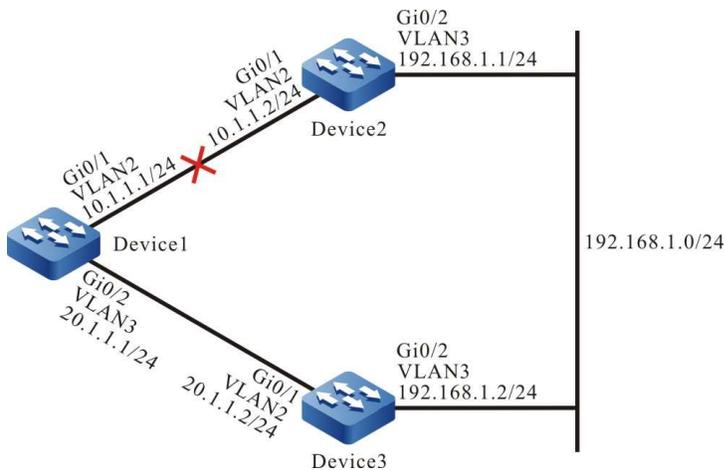


Figure 51 Network Topology for Configuring Static Floating Route

## Configuration Steps

Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configures IP addresses for the ports. (Omitted)

Step 3: Configure static routes.

#Enable Device1 to pass through Device2 and Device3 towards the network segment 192.168.1.0/24.

```
Device1#configure terminal
Device1(config)#ip route 192.168.1.0 255.255.255.0 10.1.1.2
Device1(config)#ip route 192.168.1.0 255.255.255.0 20.1.1.2
```

#View the routing table of Device1.

```
Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 10.1.1.0/24 is directly connected, 02:16:43, vlan2
C 20.1.1.0/24 is directly connected, 03:04:15, vlan3
C 127.0.0.0/8 is directly connected, 14:53:00, lo0
S 192.168.1.0/24 [1/100] via 10.1.1.2, 00:00:05, vlan2
  [1/100] via 20.1.1.2, 00:00:02, vlan3
```

It can be seen that there are two routes that can get to the network segment 192.168.1.0/24 on Device1, reaching load balancing.

Step 4: Configure floating route.

#Configure Device1. Modify the gateway as 20.1.1.2 and make the administrative distance of the route 15 so that it can become a floating route.

```
Device1(config)#ip route 192.168.1.0 255.255.255.0 20.1.1.2 15
```

Step 5: Check the result.

#View the routing table of Device1.

```
Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 10.1.1.0/24 is directly connected, 02:28:25, vlan2
C 20.1.1.0/24 is directly connected, 03:15:58, vlan3
C 127.0.0.0/8 is directly connected, 15:04:42, lo0
S 192.168.1.0/24 [1/100] via 10.1.1.2, 00:11:47, vlan2
```

According to the routing table, since the route with an administrative distance of 1 comes before the route with an administrative distance of 15, the route with a gateway of 20.1.1.2 is deleted.

#When the lines between Device1 and Device2 fail, view the routing table of Device1.

```
Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 20.1.1.0/24 is directly connected, 03:23:44, vlan3
C 127.0.0.0/8 is directly connected, 15:12:28, lo0
S 192.168.1.0/24 [15/100] via 20.1.1.2, 00:00:02, vlan3
```

The routing table indicates that the route with a larger administrative distance will be added into the routing table to be forwarded by Device3.

---

## Note

- Route backup is the most important feature of static floating route.
- 

### 51.3.3 Configure static Null0 interface route

#### Network Requirements

- Configure a static default route on Device1 and Device2 respectively. The gateway address is the address of the interface address of the peer ports of the 2 devices. Configure a static Null0 interface route for Device1 to filter the data leading to PC2 only.

#### Network Topology

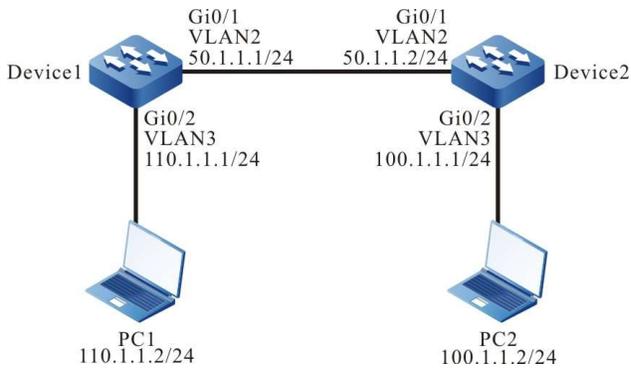


Figure 1 Network Topology for Configuring Static Null0 Interface Route

### Configuration Steps

Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configures IP addresses for the ports. (Omitted)

Step 3: Configure static routes.

#### #Configure Device1.

```
Device1#configure terminal
Device1(config)#ip route 0.0.0.0 0.0.0.0 50.1.1.2
```

#### #Configure Device2.

```
Device2#configure terminal
Device2(config)#ip route 0.0.0.0 0.0.0.0 50.1.1.1
```

#### #On PC1, use the **ping** command to verify the connectivity with PC2.

```
C:\Documents and Settings\Administrator>ping 100.1.1.2

Pinging 100.1.1.2 with 32 bytes of data:

Reply from 100.1.1.2: bytes=32 time<1ms TTL=126

Ping statistics for 100.1.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Step 4: Configure static Null0 interface route.

#### #Configure Device1.

```
Device1(config)#ip route 100.1.1.2 255.255.255.255 null0
```

Step 5: Check the result.

#View the routing table of Device1.

```
Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

S 0.0.0.0/0 [1/100] via 50.1.1.2, 00:07:28, vlan2
C 50.1.1.0/24 is directly connected, 00:07:34, vlan2
C 110.1.1.0/24 is directly connected, 00:00:08, vlan3
C 127.0.0.0/8 is directly connected, 11:46:35, lo0
S 100.1.1.2/32 [1/1] is directly connected, 00:02:31, null0
```

The static Null0 interface route has been added to the routing table.

#On PC1, use the ping command to verify the connectivity with PC2.

```
C:\Documents and Settings\Administrator>ping 100.1.1.2

Pinging 100.1.1.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 100.1.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)
```

After looking up in the routing table on Device1, the ICMP packet sent by PC1 which finds that the output interface is Null0 will be directly discarded. Therefore, PC1 cannot communicate with PC2.

---

## Note

- Static Null0 interface route is a special route. The data packets sent to this Null0 interface are all discarded. Therefore, configuring static Null0 interface route can realize packet filtering.
- 

### 51.3.4 Configure static recursive route

#### Network Requirements

- On Device1, configure two static routes leading to the network segment 192.168.1.1/32, one through Device2 and the other through Device3. Device1 prefers to use the lines between it and Device3 to forward packets.
- On Device1, configure a static recursive route leading to the network segment 200.0.0.0/24. The gateway address is the loopback interface address 192.168.1.1 of Device3. After the lines between Device1 and Device3 fail, this route will switch to Device2 for communication.

## Network Topology

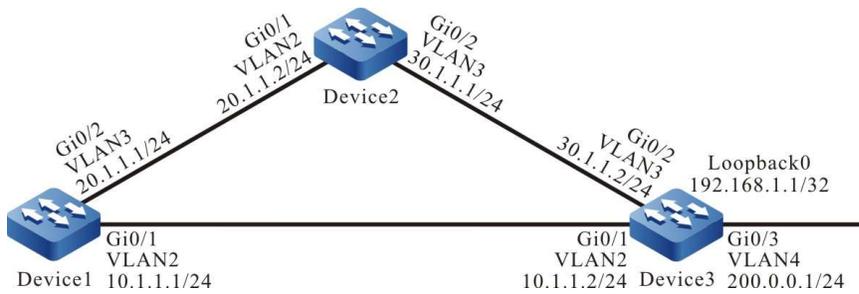


Figure 2 Network Topology for Configuring Static Recursive Route

### Configuration Steps

Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configures IP addresses for the ports. (Omitted)

Step 3: Configure static routes.

#### #Configure Device1.

```
Device1#configure terminal
Device1(config)#ip route 192.168.1.1 255.255.255.255 10.1.1.2
Device1(config)#ip route 192.168.1.1 255.255.255.255 20.1.1.2 10
```

#### #Configure Device2.

```
Device2#configure terminal
Device2(config)#ip route 192.168.1.1 255.255.255.255 30.1.1.2
```

Step 4: Configure static recursive route.

#### #Configure Device1.

```
Device1(config)#ip route 200.0.0.0 255.255.255.0 192.168.1.1
```

#### #View the routing table of Device1.

```
Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 10.1.1.0/24 is directly connected, 00:04:07, vlan2
C 20.1.1.0/24 is directly connected, 00:03:58, vlan3
C 127.0.0.0/8 is directly connected, 73:10:12, lo0
S 200.0.0.0/24 [1/100] via 192.168.1.1, 00:00:08, vlan2
S 192.168.1.1/32 [1/100] via 10.1.1.2, 00:01:46, vlan2
```

The routing table indicates that the gateway address of the route 200.0.0.0/24 is 192.168.1.1, and the output interface is VLAN2. This route depends on the route 192.168.1.1/32.

Step 5: Check the result.

#When the lines between Device1 and Device3 fail, view the routing table of Device1.

```
Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 20.1.1.0/24 is directly connected, 00:09:04, vlan3
C 127.0.0.0/8 is directly connected, 73:15:18, lo0
S 200.0.0.0/24 [1/100] via 192.168.1.1, 00:00:02, vlan3
S 192.168.1.1/32 [10/100] via 20.1.1.2, 00:00:02, vlan3
```

By comparing with the routing table mentioned in step 3, you will find that the output interface of the route 200.0.0.0/24 is VLAN3, which means it has switched to Device2 for communication.

### 51.3.5 Configure a Static Route to Coordinate with BFD

#### Network Requirements

- On Device1, configure two static routes leading to the network segment 201.0.0.0/24, one through Device2 and the other through Device3. Device1 prefers to use the lines between it and Device3 to forward packets. Likewise, configure two static routes leading to the network segment 200.0.0.0/24 on Device3 which prefers to use the lines between it and Device1 to forward packets.
- Configure static route on Device1 and Device3 to coordinate with BFD. When the lines between Device1 and Device3 fail, it will quickly switch to Device2 for communication.

#### Network Topology

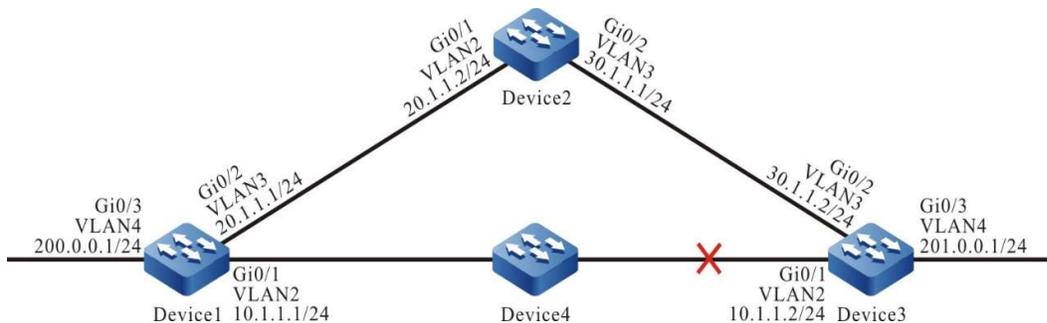


Figure 3 Network Topology for Configuring Coordination of Static Route with BFD

#### Configuration Steps

- Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)
- Step 2: Configures IP addresses for the ports. (Omitted)
- Step 3: Configure static routes.

#On Device1, configure two static routes leading to the network segment 201.0.0.0/24.

```
Device1#configure terminal
Device1(config)#ip route 201.0.0.0 255.255.255.0 vlan2 10.1.1.2
Device1(config)#ip route 201.0.0.0 255.255.255.0 vlan3 20.1.1.2 10
```

#On Device2, configure static route leading to network segments 200.0.0.0/24 and 201.0.0.0/24.

```
Device2#configure terminal
Device2(config)#ip route 200.0.0.0 255.255.255.0 20.1.1.1
Device2(config)#ip route 201.0.0.0 255.255.255.0 30.1.1.2
```

#On Device3, configure two static routes leading to the network segment 200.0.0.0/24.

```
Device3#configure terminal
Device3(config)#ip route 200.0.0.0 255.255.255.0 vlan2 10.1.1.1
Device3(config)#ip route 200.0.0.0 255.255.255.0 vlan3 30.1.1.1 10
```

#View the routing table of Device1.

```
Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 10.1.1.0/24 is directly connected, 00:07:41, vlan2
C 20.1.1.0/24 is directly connected, 00:07:29, vlan3
C 127.0.0.0/8 is directly connected, 101:56:14, lo0
C 200.0.0.0/24 is directly connected, 00:15:33, vlan4
S 201.0.0.0/24 [1/100] via 10.1.1.2, 00:02:23, vlan2
```

#Check the routing table of Device3.

```
Device3#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 10.1.1.0/24 is directly connected, 00:10:21, vlan2
C 30.1.1.0/24 is directly connected, 00:10:09, vlan3
C 127.0.0.0/8 is directly connected, 126:44:08, lo0
S 200.0.0.0/24 [1/100] via 10.1.1.1, 00:06:12, vlan2
C 201.0.0.0/24 is directly connected, 00:20:37, vlan4
```

Step 4: Configure static route to coordinate with BFD.

#Configure Device1.

```
Device1(config)#bfd fast-detect
Device1(config)#ip route static bfd vlan2 10.1.1.2
```

#Configure Device3.

```
Device3(config)#bfd fast-detect
Device3(config)#ip route static bfd vlan2 10.1.1.1
```

Step 5: Check the result.

#View the BFD session of Device1.

```

Device1#show bfd session
OurAddr      NeighAddr      LD/RD      State      Holddown      interface
10.1.1.1      10.1.1.2      15/22      UP         5000          vlan2

```

#View the BFD session of Device3.

```

Device3#show bfd session
OurAddr      NeighAddr      LD/RD      State      Holddown      interface
10.1.1.2      10.1.1.1      22/15      UP         5000          vlan2

```

The BFD sessions on Device1 and Device3 are properly established, which means the static route has been successively coordinate with BFD.

#When the lines between Device1 and Device3 fail, the BFD will quickly identify these failures and switch to Device2 for communication. View the BFD session and routing table of Device1.

```

Device1#show bfd session
OurAddr      NeighAddr      LD/RD      State      Holddown      interface
10.1.1.1      10.1.1.2      15/0       DOWN       5000          vlan2

```

```

Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

```

```

C 10.1.1.0/24 is directly connected, 00:29:07, vlan2
C 20.1.1.0/24 is directly connected, 00:28:55, vlan3
C 127.0.0.0/8 is directly connected, 102:17:40, lo0
C 200.0.0.0/24 is directly connected, 00:36:58, vlan4
S 201.0.0.0/24 [10/100] via 20.1.1.2, 00:00:09, vlan3

```

On Device3, the BFD is processed in a manner which is similar to that on Device1.

### 51.3.6 Configure static route FRR

#### Network Requirements

- On Device1, configure two static routes leading to the network segment 192.168.1.1/32, one through Device2 and the other through Device3. Device1 prefers to use the lines between it and Device3 to forward packets. Likewise, configure two static routes leading to the network segment 100.1.1.1/32 on Device3 which prefers to use the lines between it and Device1 to forward packets.
- Enable static route FRR on Device1 and Device3. When the lines between Device1 and Device3 fail, the service can quickly switch to Device2 for communication.

#### Network Topology

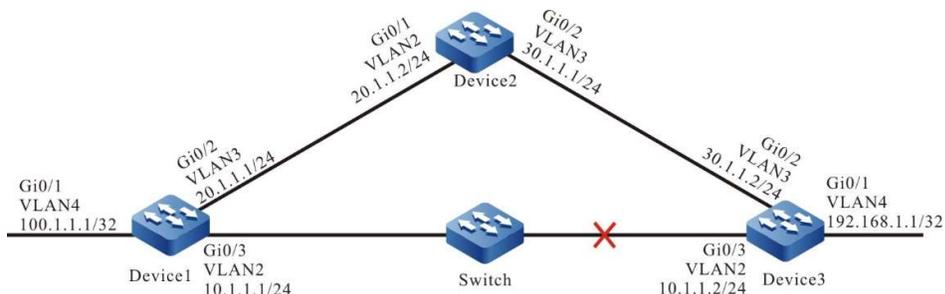


Figure 4 Network Topology for Configuring Static Route FRR

### Configuration Steps

Step 1: Configure VLAN, and add ports to the required VLAN; configure the IP address of each interface (Omitted).

Step 2: Configure static routes.

#On Device1, configure two static routes leading to 192.168.1.1/32. In particular, the administrative distance of the route with a gateway of 20.1.1.2 is 10 so that it can become a floating route.

```
Device1#configure terminal
Device1(config)#ip route 192.168.1.1 255.255.255.255 vlan 2 10.1.1.2
Device1(config)#ip route 192.168.1.1 255.255.255.255 vlan 3 20.1.1.2 10
```

#On Device2, configure the static routes leading to 100.1.1.1/32 and 192.168.1.1/32.

```
Device2#configure terminal
Device2(config)#ip route 192.168.1.1 255.255.255.255 30.1.1.2
Device2(config)#ip route 100.1.1.1 255.255.255.255 20.1.1.1
```

#On Device3, configure two static routes leading to 100.1.1.1/32. In particular, the administrative distance of the route with a gateway of 30.1.1.1 is 10 so that it can become a floating route.

```
Device3#configure terminal
Device3(config)#ip route 100.1.1.1 255.255.255.255 vlan 2 10.1.1.1
Device3(config)#ip route 100.1.1.1 255.255.255.255 vlan 3 30.1.1.1 10
```

Step 3: Configure routing policy.

#On Device1, configure route-map to invoke ACL to match 192.168.1.1/32 only, and filter other networks. The route matching the match rule applies the backup next hop interface vlan3. The next hop address is 20.1.1.2.

```
Device1(config)#ip access-list standard 1
Device1(config-std-nacl)#permit 192.168.1.1 0.0.0.0
Device1(config-std-nacl)#exit
Device1(config)#route-map ipfrr_static
Device1(config-route-map)#match ip address 1
Device1(config-route-map)#set fast-reroute backup-interface vlan3 backup-nexthop 20.1.1.2
Device1(config-route-map)#exit
```

#On Device3, configure route-map to invoke ACL to match 100.1.1.1/32 only, and filter other networks. The route matching the match rule applies the backup next hop interface vlan3. The next hop address is 30.1.1.1.

```
Device3(config)#ip access-list standard 1
Device3(config-std-nacl)#permit 100.1.1.1 0.0.0.0
Device3(config-std-nacl)#exit
Device3(config)#route-map ipfrr_static
Device3(config-route-map)#match ip address 1
Device3(config-route-map)#set fast-reroute backup-interface vlan3 backup-nexthop 30.1.1.1
Device3(config-route-map)#exit
```

Step 4: Configure FRR.

#On Device1, enable static route FRR.

```
Device1(config)#ip route static fast-reroute route-map ipfrr_static
```

#On Device3, enable static route FRR.

```
Device3(config)#ip route static fast-reroute route-map ipfrr_static
```

Step 5: Check the result.

#View the routing table of Device1.

```
Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
C 10.1.1.0/24 is directly connected, 00:31:17, vlan2
L 10.1.1.1/32 is directly connected, 00:31:17, vlan2
C 20.1.1.0/24 is directly connected, 00:08:43, vlan3
L 20.1.1.1/32 is directly connected, 00:08:43, vlan3
C 127.0.0.0/8 is directly connected, 24:43:25, lo0
L 127.0.0.1/32 is directly connected, 24:43:25, lo0
LC 100.1.1.1/32 is directly connected, 00:00:03, vlan 4
S 192.168.1.1/32 [1/10] via 10.1.1.2, 00:19:12, vlan2
```

#The FRR table of Device1 shows the route of network 192.168.1.1/32. The next hop interface is gigabitethernet0/2/1.

```
Device1#show ip frr route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
S 192.168.1.1/32 [1/10] via 20.1.1.2, 00:00:10, vlan3
```

#According to the backup next hop information of Device1, the backup interface of FRR is vlan3.

```
Device1#show nexthop frr detail

Index          : 223
Type           : FRR
Reference Count : 1
Active Path    : master
Nexthop Address : 10.1.1.2
Interface      : vlan2
Interface Vrf   : global
Channel ID     : 10
Link Header Length : 18
Link Header    : 00017a123453201201010101810000010800
Action        : FORWARDING
Slot          : 0
BK Nexthop Address : 20.1.1.2
BK Interface    : vlan3
BK Interface Vrf : global
BK Channel ID   : 11
BK Link Header Length : 18
BK Link Header  : 00017a455449201201010102810000020800
BK Action      : FORWARDING
BK Slot        : 0
```

Total 1 entries.

#When the lines between Device1 and Device3 fail, it will quickly identify the failures and switch to Device2 for communication. It can be seen from the routing table and FRR table of Device1 that the output interface of the destination network 192.168.1.1/32 in the routing table has switched to the backup interface vlan3.

```
Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 10.1.1.0/24 is directly connected, 00:31:17, vlan2
L 10.1.1.1/32 is directly connected, 00:31:17, vlan2
C 20.1.1.0/24 is directly connected, 00:08:43, vlan3
L 20.1.1.1/32 is directly connected, 00:08:43, vlan3
C 127.0.0.0/8 is directly connected, 24:43:25, lo0
L 127.0.0.1/32 is directly connected, 24:43:25, lo0
LC 100.1.1.1/32 is directly connected, 00:00:03, vlan 4
S 192.168.1.1/32 [10/10] via 20.1.1.2, 00:00:12, vlan3
```

On Device3, it is processed in a manner which is similar to that on Device1.

# 52 IPv6 Static Route

## 52.1 Overview

The IPv6 static routing protocol has the same protocol behaviors as the static routing protocol except for the IP address structure in the packet. For details, see the overview of static route.

## 52.2 IPv6 static routing function configuration

Table 52 IPv6 Static Routing Function Configuration List

Configuration Task	
Configure IPv6 static route	Configure IPv6 static route
Configure IPv6 load balancing route	Configure IPv6 load balancing route
Configure IPv6 floating route	Configure IPv6 floating route

Configuration Task	
Configure IPv6 static route to coordinate with Track	Configure IPv6 static route to coordinate with Track
Configure IPv6 static route FRR	Configure IPv6 static route FRR

### 52.2.1 Configure IPv6 static route

#### Configuration Condition

Before configuring IPv6 static route, ensure that:

- The link layer protocol has been configured to ensure normal communication at the link layer.
- Configure the IPv6 address of interface so that neighbor nodes are reachable at the network layer.

#### Configure IPv6 static route

According to the parameters that have been specified, IPv6 static routes are categorized into the following three types:

- Interface route: For an interface route, only the output interface is specified.
- Gateway route: For a gateway route, only the gateway address is specified.
- Interface gateway route: For an interface gateway route, both the output interface and the gateway address are specified.

Configured IPv6 static routes become invalid if some of the following conditions are met:

- 1) The destination address is the local interface address.
- 2) The administrative distance of the route is 255;
- 3) The output interface of the route is DOWN;
- 4) The output interface of the route doesn't enable IPv6;
- 5) The gateway address is not reachable;
- 6) The gateway address conflicts with local address;
- 7) The output interface and the gateway of the route conflict.
- 8) The output interface of the route does not exist.
- 9) The TRACK object that is associated with the route is "fake".
- 10) The status of the BFDv6 session that is associated with the route is DOWN.

If an interface route meets any one condition among 1), 2), 3), 4), 8), 9), and 10), the route is invalid. If a gateway route meets any one condition among 1), 2), 5), 6), 9), and 10), the route is invalid. If an interface gateway route meets any of the above conditions, the route is invalid.

Table 52 Configuring IPv6 Static Route

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure IPv6 static route	<b>ipv6 route destination-ipv6-address/destination-mask { interface-name / [ nexthop-ipv6-address ] } [ name nexthop-name ] [ tag tag-value ] [ track track-id ] [ administrative-distance ]</b>	Mandatory  <i>Administrative-distance</i> is the administrative distance of the static route. When it is not specified, the default value is used.

### Note

- When configuring the default route, both destination network and mask should be 0::/0.
- The output interface of Null0 route should be configured as Null0.
- No IPv6 address is required for the output interface of Null0 route.

## 52.2.2 Configure IPv6 load balancing route

### Configuration Condition

None

### Configure IPv6 load balancing route

IPv6 load balancing route means that multiple routes are configured to the same destination network. The output interfaces and the gateway addresses of the routes are different, but the administrative distances (priorities) of the routes are the same. Load balancing routes help to improve the link utility rate.

Table 1 Configuring IPv6 Load Balancing Route

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Configure the first IPv6 load balancing route	<b>ipv6 route</b> <i>destination-ipv6-address/destination-mask interface-name1 distance</i>	Mandatory The output interface is <i>interface-name1</i> .
Configure the second IPv6 load balancing route	<b>ipv6 route</b> <i>destination-ipv6-address/destination-mask interface-name2 distance</i>	Mandatory The output interface is <i>interface-name2</i> .

### Note

- When configuring the load balancing route, the distance values should be equal.

## 52.2.3 Configure IPv6 floating route

### Configuration Condition

None

### Configure IPv6 floating route

IPv6 floating static route means that multiple routes are available to the same destination network. The output interfaces or gateway addresses of the routes are different, and the priorities of the routes are also different. The route with the higher priority becomes the primary route while the route with the lower priority becomes the floating route. In the routing table, only the primary route is visible. The floating table appears in the routing table only when the primary route becomes invalid. Therefore, the floating route is usually used as a backup route.

Table 2 Configuring Floating Route

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure IPv6 preferred route	<b>ipv6 route</b> <i>destination-ipv6-address/destination-mask interface-name1 distance1</i>	Mandatory The output interface of preferred route is <i>interface-name1</i> , and the priority is <i>distance1</i> .

Step	Command	Description
Configure IPv6 floating route	<b>ipv6 route</b> <i>destination-ipv6-address/destination-mask interface-name2 distance2</i>	Mandatory  The output interface of the floating route is <i>interface-name2</i> , and the priority is <i>distance2</i> . The value of <i>distance2</i> should be greater than <i>distance1</i> .

---

### Note

- For the priority of the specified route, the smaller the distance value, the higher the priority.
- 

## 52.2.4 Configure IPv6 static route to coordinate with Track

### Configuration Condition

None

### Configure IPv6 static route to coordinate with Track

Some modules in the system need to monitor some system information and then determine their working modes based on the information. The objects that are monitored by the other modules are called monitoring objects. To simplify the relations between the modules and monitoring objects, Track objects are used. A Track object can contain multiple monitoring objects, and it displays the comprehensive status of the monitoring object to external modules. The external modules are associated only with Track objects and they do not care about monitoring objects contained in the Track objects any more. A Track object has two statuses, "true" and "false". The external modules that are associated with the Track object determine its working modes according to the Track object status.

A static route can associate with a Track object to monitor system information and determine whether the route is valid according to the status reported by the Track object. If the Track object reports "true", the conditions required by the static route are satisfied, and the route is added to the routing table. If the Track object reports "false", the route is deleted from the routing table.

Table 3 Configuring Coordination of IPv6 Static Route with TRACK

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Create Track object and enter its configuration mode	<b>track</b> <i>track-id</i>	Mandatory
Configure the link status of the specified interface for Track object monitoring	<b>interface</b> <i>interface-name</i> <b>line-protocol</b>	Optional
Return to the global configuration mode	<b>exit</b>	-
Configure a IPv6 static route and associate with Track	<b>ipv6 route</b> <i>destination-ipv6-address/destination-mask interface-name</i> <b>track</b> <i>track-id</i>	Mandatory When the link layer of the monitoring interface is UP, the route takes effect; otherwise, it becomes invalid.

## 52.2.5 Configure IPv6 static route FRR

### Configuration Condition

Before configuring IPv6 static route FRR, ensure that:

- When the FRR based on route-map is configured, the associated route-map has been configured.

### Configure static route FRR

In the network using IPv6 static route, the traffic interruption caused by link or device failure will continue until the protocol detects the link failure. It recovers only after the floating route takes effect in several seconds. Static route FRR can reduce the time of traffic interruption. By applying the routing map, set a backup next hop for the successfully matched route. Once the main link fails, the traffic passing through the main link will immediately switch to the backup link, achieving the purpose of fast switching.

Table 4 Configuring IPv6 Static Route FRR

To...	Command	Description
Enter the system	<b>configure terminal</b>	-

To...	Command	Description
configuration mode		
Configure the route-map-based FRR of static route	<b>ipv6 route static fast-reroute route-map <i>map-name</i></b>	Mandatory By default, the FRR is disabled.
Configure automatic FRR of static route	<b>ipv6 route static pic</b>	Mandatory By default, the automatic FRR is disabled.

---

### Note

- FRR is applicable to the static route with the output interface and gateway address specified at the same time only.
  - When the FRR based on route-map set backup-nexthop is auto, the protocol enables automatic FRR.
  - When pic method is used, the protocol enables automatic FRR.
  - The methods of enabling FRR are mutually exclusive.
- 

## 52.2.6 IPv6 static route monitoring and maintaining

Table 52 IPv6 Static Routing Monitoring and Maintaining

Command	Description
<b>show ipv6 route [ vrf vrf-name] static</b>	Show the static route in the IPv6 routing table
<b>show ipv6 static route [ipv6-address/mask-length]</b>	Show the IPv6 static route
<b>show running-config ipv6 route</b>	Show the configuration information of IPv6 static route

## 52.3 Typical configuration example of IPv6 static route

### 52.3.1 Configure basic functions of IPv6 static route

#### Network Requirements

- Configure IPv6 static routes for Device1, Device2 and Device3 to achieve intercommunication between PC1 and PC2.

#### Network Topology



Figure 52 Network Topology for Configuring Basic Functions of IPv6 Static Route

#### Configuration Steps

- Step 1: Configure VLAN. And add ports to the required VLAN. (Omitted)
- Step 2: Configure IPv6 addresses for the ports. (Omitted)
- Step 3: Configure IPv6 static route.

#### #Configure IPv6 route on Device1.

```
Device1#configure terminal
Device1(config)#ipv6 route 2001:4::/64 2001:2::2
```

#### #Configure Device2.

```
Device2#configure terminal
Device2(config)#ipv6 route 2001:1::/64 2001:2::1
Device2(config)#ipv6 route 2001:4::/64 2001:3::2
```

#### #Configure IPv6 route on Device3.

```
Device3#configure terminal
Device3(config)#ipv6 route 2001:1::/64 2001:3::1
```

#### #View the IPv6 routing table of Device1.

```
Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
U - Per-user Static route
O - OSPF, OE-OSPF External, M - Management

S 2001:4::/64 [1/10]
  via 2001:2::2, 00:03:14, vlan3
```

```

L ::1/128 [0/0]
  via ::, 2w0d:01:09:06, lo0
C 2001:1::/64 [0/0]
  via ::, 00:25:55, vlan2
L 2001:1::1/128 [0/0]
  via ::, 00:25:53, lo0
C 2001:2::/64 [0/0]
  via ::, 04:01:46, vlan3
L 2001:2::1/128 [0/0]
  via ::, 04:01:45, lo0

```

#### #View the IPv6 routing table of Device 2.

```

Device2#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
  via ::, 5w2d:23:52:04, lo0
S 2001:1::/64 [1/10]
  via 2001:2::1, 00:02:56, vlan2
C 2001:2::/64 [0/0]
  via ::, 04:00:52, vlan2
L 2001:2::2/128 [0/0]
  via ::, 04:00:50, lo0
C 2001:3::/64 [0/0]
  via ::, 04:00:20, vlan3
L 2001:3::1/128 [0/0]
  via ::, 04:00:19, lo0
S 2001:4::/64 [1/10]
  via 2001:3::2, 00:02:36, vlan3

```

#### # Check the IPv6 routing table of Device3.

```

Device3#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

S 2001:1::/64 [1/10]
  via 2001:3::1, 00:00:08, vlan2
L ::1/128 [0/0]
  via ::, 1w2d:20:54:36, lo0
C 2001:3::/64 [0/0]
  via ::, 03:58:28, vlan2
L 2001:3::2/128 [0/0]
  via ::, 03:58:26, lo0
C 2001:4::/64 [0/0]
  via ::, 00:11:13, vlan3
L 2001:4::1/128 [0/0]
  via ::, 00:11:12, lo0

```

Step 4: Check the result. Use the ping command to check the connectivity between PC1 and PC2.

#### #Use the ping command to check connectivity on PC1.

```

C:\Documents and Settings\Administrator>ping 2001:4::2

Pinging 2001:4::2 with 32 bytes of data:

Reply from 2001:4::2: bytes=32 time<1ms TTL=128

Ping statistics for 2001:4::2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

```

PC1 and PC2 can communicate with each other.

### 52.3.2 Configure IPv6 static floating route

#### Network Requirements

- On Device1, configure two static routes leading to the network segment 2001:3::/64, one through Device2 and the other through Device3.
- Device1 prefers to use the line between it and Device2 to forward packets; when this line fails, it will switch to Device3 for communication.

#### Network Topology

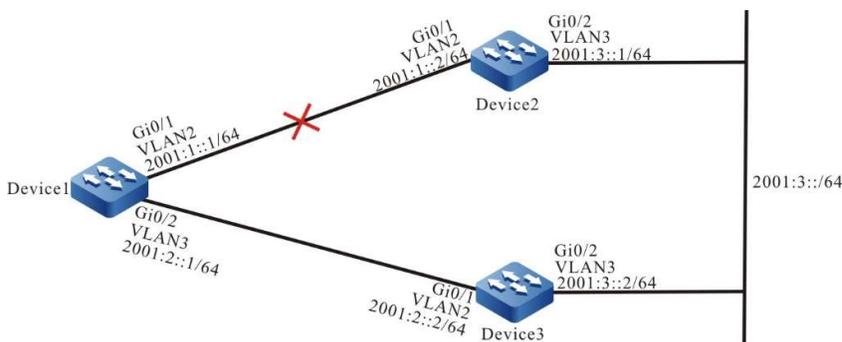


Figure 52 Network Topology for Configuring IPv6 Static Floating Route

#### Configuration Steps

- Step 1: Configure VLAN. And add ports to the required VLAN. (Omitted)
- Step 2: Configure IPv6 addresses for the ports. (Omitted)
- Step 3: Configure IPv6 static route.

#Enable Device1 to pass through Device2 and Device3 towards the network segment 2001:3::/64.

```
Device1#configure terminal
Device1(config)#ipv6 route 2001:3::/64 2001:1::2
Device1(config)#ipv6 route 2001:3::/64 2001:2::2
```

#View the IPv6 routing table of Device1.

```
Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
  via ::, 2w0d:02:13:16, lo0
C 2001:1::/64 [0/0]
  via ::, 00:22:33, vlan2
L 2001:1::1/128 [0/0]
  via ::, 00:22:32, lo0
C 2001:2::/64 [0/0]
  via ::, 00:17:47, vlan3
```

```

L 2001:2::1/128 [0/0]
  via ::, 00:17:46, lo0
S 2001:3::/64 [1/10]
  via 2001:1::2, 00:01:47, vlan2
  [1/10]
  via 2001:2::2, 00:01:36, vlan3

```

According to the result, there are two routes that can get to the network segment 2001:3::/64 on Device1, reaching load balancing.

Step 4: Configure IPv6 floating route.

#Configure Device1. Modify the gateway as 2001:2::2 and make the administrative distance of the route 15 so that it can become a floating route.

```
Device1(config)#ipv6 route 2001:3::/64 2001:2::2 15
```

Step 5: Check the result.

#View the IPv6 routing table of Device1.

```

Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
  via ::, 2w0d:02:16:38, lo0
C 2001:1::/64 [0/0]
  via ::, 00:25:56, vlan2
L 2001:1::1/128 [0/0]
  via ::, 00:25:55, lo0
C 2001:2::/64 [0/0]
  via ::, 00:21:10, vlan3
L 2001:2::1/128 [0/0]
  via ::, 00:21:09, lo0
S 2001:3::/64 [1/10]
  via 2001:1::2, 00:05:10, vlan2

```

According to the IPv6 routing table, since the route with an administrative distance of 1 comes before the route with an administrative distance of 15, the route with a gateway of 2001:2::2 is deleted.

#When the lines between Device1 and Device2 fail, view the routing table of Device1.

```

Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
  via ::, 2w0d:02:21:06, lo0
C 2001:2::/64 [0/0]
  via ::, 00:25:38, vlan3
L 2001:2::1/128 [0/0]
  via ::, 00:25:37, lo0
S 2001:3::/64 [15/10]
  via 2001:2::2, 00:00:05, vlan3

```

According to the IPv6 routing table, the route with a larger administrative distance will be added into the routing table to be forwarded by Device3.

---

## Note

- Route backup is the most important feature of static floating route.
- 

### 52.3.3 Configure IPv6 static NULL0 interface route

#### Network Requirements

- Configure a static default route on Device1 and Device2 respectively. The gateway address is the address of the interface address of the peer ports of the 2 devices. Configure a static Null0 interface route for Device1 to filter the data leading to PC2.

#### Network Topology

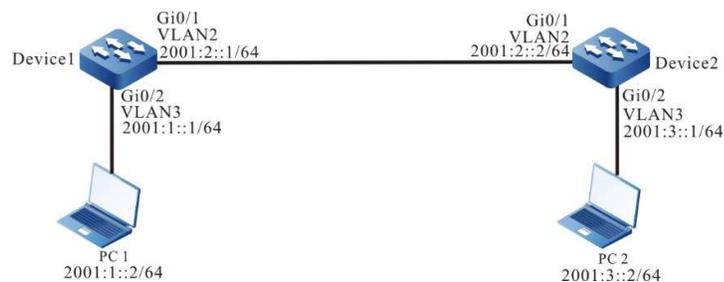


Figure 1 Network Topology for Configuring IPv6 Static NULL0 Interface Route

#### Configuration Steps

- Step 1: Configure VLAN. And add ports to the required VLAN. (Omitted)
- Step 2: Configure IPv6 addresses for the ports. (Omitted)
- Step 3: Configure IPv6 static route.

#### #Configure Device1.

```
Device1#configure terminal
Device1(config)#ipv6 route ::0 2001:2::2
```

#### #Configure Device2.

```
Device2#configure terminal
Device2(config)#ipv6 route ::0 2001:2::1
```

#### #Use the ping command to check connectivity on PC1.

```
C:\Documents and Settings\Administrator>ping 2001:3::2

Pinging 2001:3::2 with 32 bytes of data:

Reply from 2001:3::2: bytes=32 time<1ms TTL=128
Reply from 2001:3::2: bytes=32 time<1ms TTL=128
Reply from 2001:3::2: bytes=32 time<1ms TTL=128
```

```
Reply from 2001:3::2: bytes=32 time<1ms TTL=128
```

```
Ping statistics for 2001:3::2:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Step 4: Configure IPv6 static Null0 interface route.

#Configure Device1.

```
Device1(config)#ipv6 route 2001:3::2/128 null0
```

Step 5: Check the result.

#View the IPv6 routing table of Device1.

```
Device1#show ipv6 route  
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS  
U - Per-user Static route  
O - OSPF, OE-OSPF External, M - Management  
  
S ::0 [1/10]  
via 2001:1::2, 00:04:55, vlan2  
L ::1/128 [0/0]  
via ::, 2w0d:03:36:10, lo0  
C 2001:1::/64 [0/0]  
via ::, 00:08:54, vlan3  
L 2001:1::1/128 [0/0]  
via ::, 00:08:53, lo0  
C 2001:2::/64 [0/0]  
via ::, 00:08:32, vlan2  
L 2001:2::1/128 [0/0]  
via ::, 00:08:30, lo0  
S 2001:3::2/128 [1/1]  
via ::, 00:00:34, null0
```

The IPv6 static Null0 interface route has been added to the IPv6 routing table.

#On PC1, use the ping command to verify the connectivity with PC2.

```
C:\Documents and Settings\Administrator>ping 2001:3::2  
Pinging 2001:3::2 with 32 bytes of data:  
Request timed out.  
Ping statistics for 2001:3::2:  
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

After looking up in the routing table on Device1, the ICMP packet sent by PC1 which finds that the output interface is Null0 will be directly discarded. Therefore, PC1 cannot communicate with PC2.

---

## Note

- Static Null0 interface route is a special route. The data packets sent to this Null0 interface are all discarded. Therefore, configuring static Null0 interface route can realize packet filtering.
-

## 52.3.4 Configure IPv6 static recursive route

### Network Requirements

- On Device1, configure two static routes leading to the network segment 192::3/128, one through Device2 and the other through Device3. Device1 prefers to use the lines between it and Device3 to forward packets.
- On Device1, configure a static recursive route leading to the network segment 2001:4::/64. The gateway address is the loopback interface address 192::3 of Device3. After the lines between Device1 and Device3 fail, this route can switch to Device2 for communication.

### Network Topology

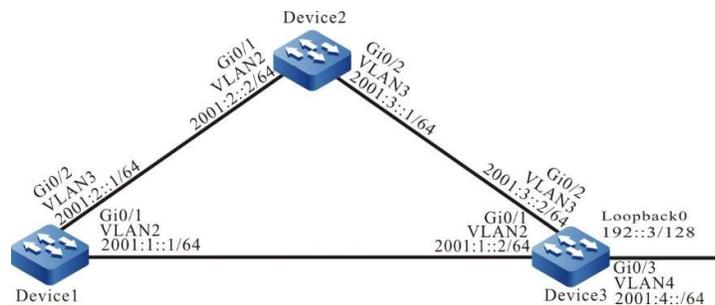


Figure 2 Network Topology for Configuring IPv6 Static Recursive Route

### Configuration Steps

- Step 1: Configure VLAN. And add ports to the required VLAN. (Omitted)
- Step 2: Configure IPv6 addresses for the ports. (Omitted)
- Step 3: Configure IPv6 static route.

#### #Configure Device1.

```
Device1#configure terminal
Device1(config)#ipv6 route 192::3/128 2001:1::2
Device1(config)#ipv6 route 192::3/128 2001:2::2 10
```

#### #Configure Device2.

```
Device2#configure terminal
Device2(config)#ipv6 route 192::3/128 2001:3::2
```

- Step 4: Configure IPv6 static recursive route.

#### #Configure Device1.

```
Device1(config)#ipv6 route 2001:4::/64 192::3
```

#### #View the IPv6 routing table of Device1.

```

Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
  via ::, 2w0d:03:12:46, lo0
S 192::3/128 [1/10]
  via 2001:1::2, 00:04:54, vlan2
C 2001:1::/64 [0/0]
  via ::, 00:22:47, vlan2
L 2001:1::1/128 [0/0]
  via ::, 00:22:45, lo0
C 2001:2::/64 [0/0]
  via ::, 00:16:16, vlan3
L 2001:2::1/128 [0/0]
  via ::, 00:16:15, lo0
S 2001:4::/64 [1/10]
  via 192::3, 00:00:43, vlan2

```

According to the IPv6 routing table, the gateway address of the route 2001:4::/64 is 192::3, and the output interface is VLAN2. This route depends on the route 192::3/128.

Step 5: Check the result.

#When the lines between Device1 and Device3 fail, view the IPv6 routing table of Device1.

```

Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
  via ::, 2w0d:03:17:48, lo0
S 192::3/128 [10/10]
  via 2001:2::2, 00:00:06, vlan3
C 2001:2::/64 [0/0]
  via ::, 00:21:18, vlan3
L 2001:2::1/128 [0/0]
  via ::, 00:21:17, lo0
S 2001:4::/64 [1/10]
  via 192::3, 00:00:06, vlan3

```

According to the routing table mentioned in step 3, the output interface of the route 2001:4::/64 is VLAN3, which means it has switched to Device2 for communication.

### 52.3.5 Configure static FRR for IPv6 static route

#### Network Requirements

- On Device1, configure two static routes leading to the network segment 1001:2::1/64, one through Device2 and the other through Device3. Device1 prefers to use the lines between it and Device2 to forward packets.
- Enable static FRR between Device1 and Device3. When the lines fail, the service can quickly switch to Device2 for communication.

#### Network Topology

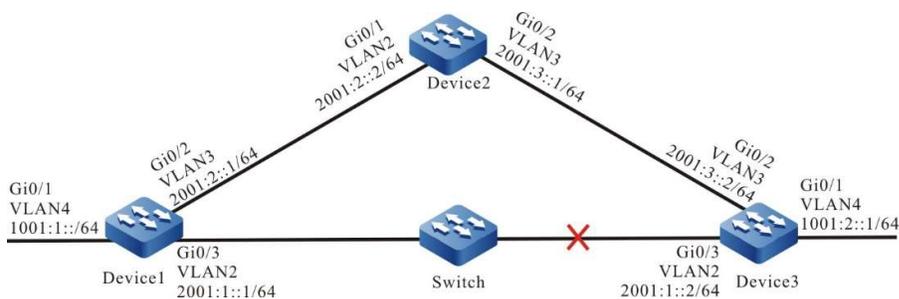


Figure 3 Network Topology for Configuring Static FRR of IPv6 Static Route

### Configuration Steps

- Step 1: Configure VLAN, and add ports to the required VLAN; configure the IPv6 address of each interface (Omitted).
- Step 2: Configure IPv6 static route.

#On Device1, configure two static routes leading to the network 1001:2::/64.

```
Device1#configure terminal
Device1(config)#ipv6 route 1001:2::/64 vlan2 2001:1::2
Device1(config)#ipv6 route 1001:2::/64 vlan3 2001:2::2 10
```

#On Device2, configure a static route leading to the network 1001:2::1/64.

```
Device2#configure terminal
Device2(config)#ipv6 route 1001:2::/64 vlan3 2001:3::2
```

- Step 3: Configure routing policy.

#On Device1, configure route-map to invoke ACL to match 1001:2::1/64 only, and filter other network segments. The route matching the match rule applies the backup next hop interface vlan3. The next hop address is 2001:2::2.

```
Device1(config)#ipv6 access-list extended 7001
Device1(config-v6-list)#permit ipv6 1001:2::1/64 any
Device1(config-v6-list)#exit
Device1(config)#route-map ipv6frr_st
Device1(config-route-map)#match ipv6 address 7001
Device1(config-route-map)#set ipv6 fast-reroute backup-interface vlan3 backup-nexthop 2001:2::2
Device1(config-route-map)#exit
```

- Step 4: Configure static FRR.

```
Device1(config)#ipv6 route static fast-reroute route-map ipv6frr_st
```

- Step 5: Check the results.

```
#View the IPv6 static routing table of Device1.
Device1#show ipv6 route
```

```

Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management
L ::1/128 [0/0]
  via ::, 04:26:25, lo0
C 1001:1::/64 [0/0]
  via ::, 04:21:32, vlan4
L 1001:1::1/128 [0/0]
  via ::, 04:21:32, vlan4
S 1001:2::/64 [1/10]
  via 2001:1::2, 00:03:00, vlan2
C 2001:1::/64 [0/0]
  via ::, 04:22:11, vlan2
L 2001:1::1/128 [0/0]
  via ::, 04:22:11, vlan2
C 2001:2::/64 [0/0]
  via ::, 04:20:50, vlan3
L 2001:2::1/128 [0/0]
  via ::, 04:20:50, vlan3

```

According to the routing table, the route 1001:2::/64 prefers the lines between Device1 and Device3 for communication.

#View the IPv6 frr routing table of Device1.

```

Device1#show ipv6 frr route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management
S 1001:2::/64 [1/4294967295]
  via 2001:2::2, 00:04:32, vlan3

```

According to the result, the next hop and output interface of the frr route 1001:2::/64 are 2001:2::2 and vlan3 respectively.

#View the BFD session information of Device1.

```

Device1#show bfd session ipv6 2001:1::2 detail
Total ipv6 session number: 1
OurAddr      NeighAddr    LD/RD        State  Holddown  Interface
2001:1::1    2001:1::1    1015/1015    UP     500       vlan2
Type:ipv6 direct Mode:echo
Local Discriminator:67 Remote Discriminator:67
Local State:UP Remote State:UP Up for: 0h:30m:28s Number of times UP:1
Send Interval:100ms Detection time:500ms(100ms*5)
Local Diag:0 Demand mode:0 Poll bit:0
Registered modules:FIB_MGR

```

According to the result, FIB\_MGR has been successfully coordinated with BFD. The session is established normally in the mode of echo.

#When the lines between Device1 and Device3 fail, it can quickly identify the failures and switch to Device2 for communication. The routing table of Device1 shows that the output interface of the destination network 1001:2::/64 has switched to the backup interface vlan3.

```

Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management
L ::1/128 [0/0]
  via ::, 04:56:34, lo0
C 1001:1::/64 [0/0]
  via ::, 04:51:41, vlan4
L 1001:1::1/128 [0/0]
  via ::, 04:51:41, vlan4
S 1001:2::/64 [10/10]

```

```

via 2001:2::2, 00:00:08, vlan3
C 2001:2::/64 [0/0]
via ::, 04:50:59, vlan3
L 2001:2::1/128 [0/0]
via ::, 04:50:59, vlan3

```

### 52.3.6 Configure dynamic FRR for IPv6 static route

#### Network Requirements

- On Device1, configure two static routes leading to the network segment 1001:2::1/64, one through Device2 and the other through Device3. Device1 prefers to use the lines between it and Device2 to forward packets.
- Enable dynamic FRR between Device1 and Device3. When the lines fail, the service can quickly switch to Device2 for communication.

#### Network Topology

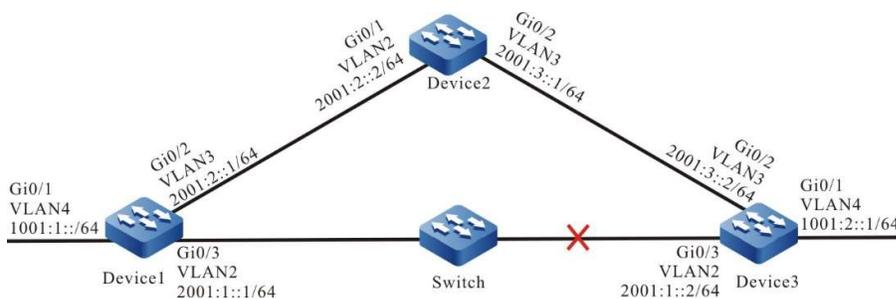


Figure 4 Network Topology for Configuring Dynamic FRR of IPv6 Static Route

#### Configuration Steps

- Step 1: Configure VLAN, and add ports to the required VLAN; configure the IPv6 address of each interface (Omitted).
- Step 2: Configure IPv6 static route.

#On Device1, configure two static routes leading to the network 1001:2::/64.

```

Device1#configure terminal
Device1(config)#ipv6 route 1001:2::/64 vlan2 2001:1::2
Device1(config)#ipv6 route 1001:2::/64 vlan3 2001:2::2 10

```

#On Device2, configure a static route leading to the network 1001:2::1/64.

```

Device2#configure terminal
Device2(config)#ipv6 route 1001:2::/64 vlan3 2001:3::2

```

- Step Configure routing policy

3:

#On Device1, configure route-map to invoke ACL to match 1001:2::1/64 only, and filter other network segments. The route matching the match rule applies the backup next hop interface vlan3. The next hop address is auto.

```
Device1(config)#ipv6 access-list extended 7001
Device1(config-v6-list)#permit ipv6 1001:2::1/64 any
Device1(config-v6-list)#exit
Device1(config)#route-map ipv6frr_st
Device1(config-route-map)#match ipv6 address 7001
Device1(config-route-map)#set ipv6 fast-reroute backup-nexthop auto
Device1(config-route-map)#exit
```

Step 4: Configure dynamic FRR.

```
Device1(config)#ipv6 route static fast-reroute route-map ipv6frr_st
```

Step 5: Check the results.

#View the IPv6 static routing table of Device1.

```
Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management
L ::1/128 [0/0]
  via ::, 04:26:25, lo0
C 1001:1::/64 [0/0]
  via ::, 04:21:32, vlan4
L 1001:1::1/128 [0/0]
  via ::, 04:21:32, vlan4
S 1001:2::/64 [1/10]
  via 2001:1::2, 00:03:00, vlan2
C 2001:1::/64 [0/0]
  via ::, 04:22:11, vlan2
L 2001:1::1/128 [0/0]
  via ::, 04:22:11, vlan2
C 2001:2::/64 [0/0]
  via ::, 04:20:50, vlan3
L 2001:2::1/128 [0/0]
  via ::, 04:20:50, vlan3
```

According to the routing table, the route 1001:2::/64 prefers the lines between Device1 and Device3 for communication.

#View the IPv6 frr routing table of Device1.

```
Device1#show ipv6 frr route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management
S 1001:2::/64 [1/4294967295]
  via 2001:2::2, 00:04:32, vlan3
```

According to the result, the next hop and output interface of the frr route 1001:2::/64 are 2001:2::2 and vlan3 respectively.

#View the BFD session information of Device1.

```
Device1#show bfd session ipv6 2001:1::1 detail
Total ipv6 session number: 1
```

```

OurAddr      NeighAddr      LD/RD      State  Holddown  Interface
2001:1::1    2001:1::1     1012/1012  UP     500       vlan2
Type:ipv6 direct Mode:echo
Local Discriminator:67 Remote Discriminator:67
Local State:UP Remote State:UP Up for: 0h:30m:28s Number of times UP:1
Send Interval:100ms Detection time:500ms(100ms*5)
Local Diag:0 Demand mode:0 Poll bit:0
Registered modules:FIB_MGR

```

According to the result, FIB\_MGR has been successfully coordinated with BFD. The session is established normally in the mode of echo.

#When the lines between Device1 and Device3 fail, it can quickly identify the failures and switch to Device2 for communication. The routing table of Device1 shows that the output interface of the destination network 1001:2::/64 has switched to the backup interface vlan3.

```

Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management
L ::1/128 [0/0]
  via ::, 04:56:34, lo0
C 1001:1::/64 [0/0]
  via ::, 04:51:41, vlan4
L 1001:1::1/128 [0/0]
  via ::, 04:51:41, vlan4
S 1001:2::/64 [10/10]
  via 2001:2::2, 00:00:08, vlan3
C 2001:2::/64 [0/0]
  via ::, 04:50:59, vlan3
L 2001:2::1/128 [0/0]
  via ::, 04:50:59, vlan3

```

# 53 RIP

---

## 53.1 Overview

On the current Internet, it is impossible to run only one gateway protocol. You can divide it into multiple Autonomous Systems (ASs), each of which has its own routing technology. The internal routing protocols within an AS are Interior Gateway Protocols (IGPs). Routing Information Protocol (RIP) is one type of IGP. RIP adopts the Vector-Distance algorithm. RIP features simple and easy-to-use, so it is widely used in numerous small-sized networks.

RIP has two versions: RIPv1 and RIPv2. RIPv1 does not support classless routing, and RIPv2 supports classless routing. Usually, RIPv2 is used.

RIP is a simple protocol which provides simple configuration. However, the number of routes to be advertised by RIP is directly proportional to the number of routes in the routing table. If the number of routes is large, a lot of device resources and network resources are consumed. In addition, RIP specifies that the maximum number of hops that a routing path that passes routers is 15, so RIP is applicable only to simple small and medium-sized network. RIP is applicable for most campus networks and LANs with a simple structure and strong continuity. For a more complex environment, RIP is not recommended.

RIPv1 was introduced earlier in RFC1058, but it has many deficiencies. To improve the deficiencies of RIPv1, RFC1388 introduced RIPv2, which was then revised in RFC 1723 and RFC 2453.

## 53.2 RIP function configuration

Table 53 RIP Function Configuration List

Configuration Task	
Configure RIP Basic Functions	Globally Enable RIP
	Enable RIP via VRF
	Configure RIP Version

Configuration Task	
Configure RIP Route Generation	Configure RIP to Distribute Default Route
	Configure RIP Route Redistribution
Configure RIP Route Control	Configure RIP Administrative Distance
	Configure RIP Route Summarization
	Configure the RIP Metric Offset
	Configure RIP Route Filtration
	Configure the Metric of the RIP Interface
	Configure the Routing Flag for an RIP Interface
Configure RIP Network Authentication	Configure the Maximum Load Balancing
	Configure RIP Network Authentication
Configure RIP Network Optimization	Configure RIP Timers
	Configure Split Horizon and Toxicity Reverse of RIP
	Configure Source Address Check
	Configure a Static RIP Neighbor
	Configure a Passive RIP Interface
	Configure RIP to Trigger Updates
	Configure an RIP Standby Interface
Configure RIP to Coordinate with BFD	Configure RIP to Coordinate with BFD

### 53.2.1 Configure RIP Basic Functions

#### Configuration Condition

Before configuring the basic functions of RIP, ensure that:

- The link layer protocol has been configured to ensure normal communication at the link layer.
- Configure address of interface at network layer so that neighbor network nodes are reachable at the network layer.

### Globally Enable RIP

To use RIP, the following configurations are required:

- Create RIP process;
- Configure RIP to cover direct network or an interface.

Table 53 Globally Enabling RIP

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Create RIP process and enter RIP configuration mode	<b>router rip</b>	Mandatory By default, RIP process is disabled.
Cover the specified network segment or interface	<b>network</b> { <i>ip-address</i>   <i>interface-name</i> }	Mandatory By default, no direct network or interface is covered.

---

### Note

- The network segment configured to cover will be automatically classified as classful address.
  - **network** *ip-address* cannot cover supernet address, but this can be done through **network** *interface-name*.
- 

### Enable RIP via VRF

RIP supports VRF function. The following configurations are required:

- Configure a VRF, and specify an interface to add into this VRF;
- Specify to enable RIP function in the address family of this VRF;

- Configure RIP to cover a VRF direct network or the interface where it belongs.

Table 1 Enabling RIP via VRF

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Create RIP process and enter RIP configuration mode	<b>router rip</b>	Mandatory By default, RIP process is disabled.
Enter the RIP VRF address family configuration mode	<b>address-family { ipv4 vrf vrf-name }</b>	Mandatory By default, the VRF address family mode is disabled.
Cover the specified network segment or interface	<b>network { ip-address   interface-name }</b>	Mandatory By default, no direct network or interface is covered.

### Note

- To enable RIP in VRF mode, VRF-related configurations must be created first.

### Configure RIP Version

RIP supports two versions, i.e. RIPv1 and RIPv2. It can be configured in three modes: global, VRF, and interface:

- By default, the RIPv1 version is enabled in global and VRF mode, and it is not configured in interface mode;
- The priority of the version command configured in interface mode is higher than that in global or VRF mode;
- When the version command is not configured in interface mode, that in VRF or global mode where the interface is located will be used;
- In interface mode, the RIP receiving and sending version can be configured separately;
- After a version is configured, RIP will implement strict packet receiving and sending rules: When RIPv1 is configured, only RIPv1 broadcast or unicast packets are sent and received; when RIPv2 is configured, RIPv2 unicast, multicast or broadcast packets are sent and

received; in RIPv1 compatible mode, RIPv2 unicast and broadcast packets are sent.

Table 53 Configuring RIP Version

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Create RIP process and enter RIP configuration mode	<b>router rip</b>	Mandatory By default, RIP process is disabled.
Configure global RIP version	<b>version { 1   2 }</b>	Mandatory By default, RIPv1 is enabled.
Enter the RIP VRF configuration mode	<b>address-family { ipv4 vrf vrf-name }</b>	Mandatory By default, the VRF address family is disabled.
Configure the RIP version in RIP VRF configuration mode	<b>version { 1 / 2 }</b>	Mandatory By default, RIPv1 is enabled.
Return to RIP configuration mode	<b>exit-address-family</b>	-
Return to global configuration mode	<b>exit</b>	-
Enter the interface configuration mode	<b>interface interface_name</b>	-
Configure the interface to send RIP version	<b>ip rip send version {{ 1 / 2 }   1-compatible }</b>	Optional By default, the packets are sent based on the RIP global version.
Configure the interface to receive RIP Version	<b>ip rip receive version { 1 / 2 }</b>	Optional By default, the packets are received based on the RIP global version.

## 53.2.2 Configure RIP Route Generation

### Configuration Condition

Before configuring RIP route generation, ensure that:

- Interface IP addresses have been configured so that neighbor nodes are reachable at the network layer.
- RIP is enabled.

### Configure RIP to Distribute Default Route

Through configuration, the device sends default routes under all RIP interfaces and sets itself as the default gateway of other adjacent devices.

Table 53 Configuring RIP to Distribute Default Route

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the RIP configuration mode	<b>router rip</b>	Mandatory By default, RIP process is disabled.
Configure RIP to Distribute Default Route	<b>default-information originate {only   originate [metric value] }</b>	Mandatory By default, RIP doesn't distribute default route.

### Note

- If a default route (0.0.0.0/0) is learned, it will replace the default route (0.0.0.0/0) distributed by the device. When there is loop in the network, route oscillation may be caused. Thus, when using this command, be sure that several other devices in the same routing domain are not enabling it at the same time.

### Configure RIP Route Redistribution

The routes generated by other protocols can be imported into RIP by configuring route redistribution.

Table 2 Configuring RIP Route Redistribution

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the RIP configuration mode	<b>router rip</b>	Mandatory By default, RIP process is disabled.
Configure the default metric value of importing other routing protocol by RIP	<b>default-metric</b> <i>metric-value</i>	Optional By default, the default metric value of importing other routing protocol is 1.
Configure RIP Route Redistribution	<b>redistribute</b> <i>protocol</i> [ <i>protocol-id</i> ] [ <b>metric</b> <i>metric-value</i> ] [ <b>route-map</b> <i>route-map-name</i> ] [ <b>match</b> <i>route-sub-type</i> ]	Mandatory By default, no route redistribution is configured.

---

### Note

- In case of redistribution, after the metric command option is specified, the route redistributed will adopt this metric value.
  - For RIP, when configuring route redistribution application routing policies, the match options supported include ip address, route type, and tag, and the set options supported include interface, ip next-hop, route source, and metric.
- 

## 53.2.3 Configure RIP Route Control

### Configuration Condition

Before configuring RIP route control, ensure that:

- Interface IP addresses have been configured so that neighbor nodes are reachable at the network layer.
- RIP is enabled.

### Configure RIP Administrative Distance

Multiple routing protocols can run in the device at the same time. The device selects the routes learned by each protocol through administrative distance. The smaller the administrative distance, the more like the route is selected.

Table3 Configuring RIP Administrative Distance

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the RIP configuration mode	<b>router rip</b>	-
Configure RIP Administrative Distance	<b>distance</b> <i>distance-value</i>	Mandatory By default, RIP administrative distance is 120.

### Configure RIP Route Summarization

RIP route summarization means the device summarizes the subnet routes in the same natural network segment into one route. The route generated by summarization and the original subnet routes are listed in the RIP routing table at the same time.

After RIP route summarization is configured, the device only advertises the summarized routes. This can significantly reduce the scale of adjacent RIP routing tables in large and medium-sized networks and the consumption of network bandwidth by routing protocol packets.

The metric of the summarized route will be the minimum metric value among all subnet routes.

RIPv1 supports automatic route summarization, and RIPv2 supports both automatic and manual route summarization.

#### 1. RIP automatic route summarization

Automatic route summarization is different from manual route summarization. It automatically generates a natural mask route according to the subnet routes within the same natural network segment.

Table 4 Configuring Automatic Route Summarization Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Enter the RIP configuration mode	<b>router rip</b>	Mandatory By default, RIP process is disabled.
Configure automatic route summarization function	<b>auto-summary</b>	Mandatory By default, the automatic route summarization function is disabled.

## Note

- RIPv1 does not allow route summarization through commands.
- The tag of the summarized route is 0, and the metric value of the route is the minimum value among the detail routes. When the automatic summarization function is configured, automatic summarization occurs first.
- For RIPv2, be careful to use the automatic route summarization function. Make ensure that automatic route summarization is necessary in the network, otherwise routing loops may be produced.
- If the automatic route summarization is enabled in RIPv2, when the interface advertises the route is in the same natural network segment as the route, the update packet sent from this interface will not summarize all the subnet routes in this natural network segment. Otherwise, the routes will be summarized into natural network segment for advertisement.

## 2. Manual route summarization

For manual route summarization, a pair of destination address and mask combination need to be configured. They will summarize the routes in the covered network segment.

Table 5 Configuring Manual Route Summarization Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-

Step	Command	Description
Configure the manual route summarization function of RIPv2 on the interface	<b>ip summary-address rip</b> <i>prefix-address</i>	-

### Configure the RIP Metric Offset

By default, RIP applies the route metric advertised by the neighbor device to the received routes. To modify the metric in some special application scenarios, you can configure the RIP metric offset to correct the metric of the specified route.

If the metric in the incoming direction is configured, RIP modifies the metric of the received routes and saves the routes into the routing table. When RIP advertises a metric to the neighbor devices, it advertises the new metric. If the metric in the outgoing direction is configured, the metric is modified only when RIP advertises a metric to the neighbor devices.

Table 6 Configuring RIP Metric Offset

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the RIP configuration mode	<b>router rip</b>	Mandatory By default, RIP process is disabled.
Configure RIP to modify the metric of the specified route	<b>offset-list</b> <i>access-list-name</i> { <b>in</b>   <b>out</b> } <i>metric-offset</i> [ <i>interface-name</i> ]	Mandatory By default, no metric value of interface is configured.

### Note

- Route metric offset supports the standard access list only.

### Configure RIP Route Filtration

A router can filter the received or advertised routes by configuring an Access Control List (ACL) or prefix list. In receiving RIP routes, you can filter some learnt routes; or in announcing RIP routes, you can filter some routes that are advertised to neighbor devices.

Table 5-11 Configuring RIP Route Filtration

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the RIP configuration mode	<b>router rip</b>	Mandatory By default, RIP process is disabled.
Configure RIP route filtration function	<b>distribute-list</b> { <i>access-list-name</i>   <b>prefix</b> <i>prefix-list-name</i> } { <b>in</b>   <b>out</b> } [ <i>interface-name</i> ]	Mandatory By default, no route filtration function is configured. When the route filtration function is configured, if an interface is not specified, route filtration will be enabled for all RIP covered interfaces during the receiving or sending process.

### Note

- When using ACL filtration, only standard ACL is supported.

### Configure the Metric of the RIP Interface

If an interface is overwritten by an RIP process, the corresponding direct route is generated in the database, with the default metric 1. When the route is in the RIP database or it is advertised to neighbor devices, if the interface is configured with a metric, the interface metric is used as the metric of the route.

If the interface metric is changed, the RIP database immediately updates the corresponding direct route of RIP and advertises the new metric to the neighbor devices.

Table 7 Configuring Metric Value of RIP Interface

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure the metric of the RIP interface	<b>ip rip metric</b> <i>metric-value</i>	Mandatory By default, the matrix value of the RIP interface is 1.

### Note

- When the matrix value of the RIP interface is configured, the matrix of the direct subnet on the interface instead of that of route learning will be affected.

### Configure the Routing Flag for an RIP Interface

The network administrator can attach tags to some routes. Then, in applying a routing policy, the network administrator can perform route filtration or route property advertisement based on the tags.

Only the routing tags of RIPv2 are supported.

Table 8 Configuring Routing Flag for RIP interface

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure the routing tag on the direct subnet on the interface of RIP	<b>ip rip tag</b> <i>tag-value</i>	-

### Configure the Maximum Number of RIP Load Balancing Entries

This command helps you to control the number of RIP load balancing entries for routing.

Table 9 Configuring Maximum Number of Load Balancing Entries of RIP

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the RIP configuration mode	<b>router rip</b>	Mandatory By default, RIP process is disabled.
Configure the Maximum Number of RIP Load Balancing Entries	<b>maximum-paths</b> <i>max-number</i>	Optional By default, the maximum number of load balancing entries of RIP is 4.

### 53.2.4 Configure RIP Network Authentication

RIPv2 supports protocol packet authentication, therefore, it can satisfy the high security requirement of some networks. Currently, plain text authentication and Message Digest 5 (MD5) authentication are supported. Plain text authentication features low security because it transmits plain text. MD5 converts an authentication code into the MD5 code for transmission, ensuring higher security.

Owing to the limit of RIPv2 packets, a packet that advertises a route contains only 16 bytes. Therefore, the length of a plain text authentication string must not exceed 16 bytes. Meanwhile, the MD5 code that is converted from any character string is a standard 16-byte code, meeting the requirement on the string length.

Table 10 Configuring RIP Network Authentication

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure RIPv2 network authentication	<b>ip rip authentication</b> { { <b>key</b> { 0   7 } <i>key-string</i> }   { <b>key-chain</b> <i>key-chain-name</i> } 	Mandatory By default, no RIPv2 authentication function is configured.

Step	Command	Description
	<code>{ mode { text   md5   sm3 } }</code>	

## Note

- Before implementing MD5 authentication, pay attention to the following points:
- RIPv1 does not support network authentication.
- RIPv2 supports one authentication mode at a time.
- Key ID must be carried in the MD5 authentication information. If you use the `ip rip authentication key` command to configure a password, the key ID is 1. If you use the `ip rip authentication key-chain` command to configure a password, the key ID is the key ID in Key-chain.
- In obtaining a packet transmit authentication password from Key-chain, select a Key ID in the sequence of from small to large. Therefore, the Key ID with the smallest valid transmit password will be selected.
- In obtaining a packet receive authentication password from Key-chain, select the first valid receive password whose Key ID is equal to or larger than the packet receive Key ID. Therefore, if Key IDs are different for the two ends of authentication, the end with the larger Key ID can pass the authentication while the end with the smaller Key ID fails in the authentication.

## 53.2.5 Configure RIP Network Optimization

### Configuration Condition

Before configuring RIP network optimization, ensure that:

- Interface IP addresses have been configured so that neighbor nodes are reachable at the network layer.
- RIP is enabled.

### Configure RIP Timers

RIP does not maintain neighbor relations and it does not support route withdrawn; therefore, the protocol provides four configurable timers to control the network convergence speed. The four timers are: route update timer, router timeout timer, route dampening update timer, and route clear timer.

The route timeout time must be at least three times of the route update time. If no route update packet is received within the route timeout time, the route becomes invalid and it enters a dampening cycle. The length of the dampening cycle is determined by the dampening update time. During the cycle, the route will not be cleared. After the dampening cycle is completed, the route enters the clear cycle. During the

cycle, the route can be updated. However, if no route update packet is received during the cycle, the route will be deleted.

Table 11 Configuring RIP Timer

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the RIP configuration mode	<b>router rip</b>	Mandatory By default, RIP process is disabled.
Configure the time of RIP timer	<b>timers basic update-interval invalid-interval holddown-interval flush-interval</b>	Optional By default, the RIP update interval is 30 seconds, the effective time of advertisement 180 seconds, the suppression time 180 seconds, and the clearing time 240 seconds.

---

### Caution

- In the same RIP routing domain, the **timer basic** configurations on all devices must be consistent to avoid network flapping.
- 

### Configure RIP Split Horizon and Toxicity Reverse of RIP

Split horizon and toxicity reverse are mechanisms that are used to prevent route loops.

1. Configure split horizon.

RIP does not advertise routes that it has learnt from an interface to the interface, preventing routing loops.

Table 12 Configuring RIP Split Horizon

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure RIP split horizon	<b>ip split-horizon</b>	Mandatory By default, the split horizon function is disabled.

## 2. Configure toxicity reverse.

RIP announces routes that have been learnt from an interface to the interface, but the route metric is the maximum number of hops, 16, preventing routing loops.

Table 13 Configuring Toxicity Reverse

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure RIP toxicity reverse	<b>ip split-horizon poisoned</b>	Optional By default, the toxicity reverse function is enabled.

### Note

- The split horizon and toxicity reverse functions are valid only for the learnt routes, direct routes in the network covered by RIP, and the redistributed direct and static routes.
- The split horizon function and the toxicity reversion function cannot be used at the same time.

## Configure RIP Source Address Check

Through source address check, RIP checks the source addresses of the received packets. RIP processes only the packets whose source addresses meet the requirements. The check items include: the packet source

address is in the same network segment as the input interface address; the packet source address matches the peer end address of the Point-to-Point (P2P) interface.

By default, RIP is enabled to check whether the source addresses received through the Ethernet port are in the same network segment as the address of the interface, and this function cannot be cancelled.

Table 14 Configuring RIP Source Address Check

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the RIP configuration mode	<b>router rip</b>	Mandatory By default, RIP process is disabled.
Configure RIP source address check on the interface of P2P	<b>validate-update-source check-p2p-destination</b>	Mandatory By default, address of peer port is not checked for P2P interface.

### Configure a Static RIP Neighbor

RIP does not maintain neighbor relations, so it does not have the concept of neighbor. Here the neighbor refers to the neighbor RIP routing device. After a static RIP neighbor is specified, RIP sends RIP packets to the neighbor in unicast mode. The configuration is applied to a network that does not support broadcast or multicast, such as point-to-point links. If the configuration is applied to a broadcast or multicast network, it may cause repeated RIP packets in the network.

Table 15 Configuring Static RIP Neighbor

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the RIP configuration mode	<b>router rip</b>	Mandatory By default, RIP process is disabled.
Configure the neighbor which advertises routing	<b>neighbor ip-address</b>	Mandatory

Step	Command	Description
information in the form of unicast		The parameter ip-address is the ip address of the direct interface of the peer port.

### Note

- The advertisement of routing information to static neighbors occurs only on the interfaces covered by RIP, and "**passive-interface**" cannot prevent them from sending packets to static neighbors.

### Configure a Passive RIP Interface

To decrease the network bandwidth consumed by the routing protocol, the dynamic routing protocol uses the passive interface function. RIP receives only route update packets on a passive interface, and it does not send route update packets on the passive interface. In a low-speed network with small bandwidth, the passive interface function and the neighbor function cooperate to effectively reduce interactions of RIP routes.

Table 16 Configuring Passive RIP Interface

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the RIP configuration mode	<b>router rip</b>	Mandatory By default, RIP process is disabled.
Configure a Passive RIP Interface	<b>passive-interface { default   interface-name }</b>	Mandatory By default, no passive interface is configured.

### Note

- The passive interface function does not restrain an interface from sending unicast route updates to its neighbor devices. When the passive interface function is used with the neighbor command, the function does not restrain an interface from sending unicast route updates to

---

its neighbor devices. This application mode controls a router so that it sends route updates only to some neighbor devices in unicast mode instead of sending route updates to all neighbor devices in broadcast mode (or multicast mode in the case of RIPv2).

---

### Configure RIP to Trigger Updates

After a device receives an RIP update packet, to reduce the possibility of introducing loops owing to routing table differences, the device advertises the update packet of the route to its neighbor devices immediately instead of waiting for the update timer to time out before an update. The update trigger mechanism speeds up network convergence.

Table 17 Configuring RIP to Trigger Updates

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure RIP to trigger updates on the interface	<b>ip rip triggered</b>	Optional By default, the trigger updates function is disabled.

### Configure an RIP Standby Interface

To speed up backup route convergence, RIP newly supports a backup interface (standby interface) function. On the main route interface of RIP, specify a backup interface for the main interface. In a specific application environment, RIP learns RIP routes only from one line, and the backup line does not provide routing information interaction. If the main interface gets offline, RIP sends Request packets to the peer end through the backup interface periodically (Default: 1s) to request for all routes. If the backup interface receives a Response packet from the peer route, RIP cancels sending of Request packets. It updates the local routing table, and advertises the local routing table to the backup interface. If the backup interface fails to receive a Response packet from the peer end before timeout, RIP cancels sending of Request packets.

Table 18 Configuring RIP Backup Interface

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure an RIP Standby Interface	<b>ip rip standby</b> <i>interface-name</i> [ <b>timeout</b> <i>timeout-value</i> ]	Optional  By default, the backup interface function is disabled, and the default value of <i>timeout-value</i> is 300s.

### 53.2.6 Configure RIP to Coordinate with BFD

The backup interface can be used in specific application environments only. It cannot meet the requirements of real-time backup. The BFD (Bidirectional Forwarding Detection) function of RIP which provides end-to-end protection can achieve rapid route convergence and switch. BFD can rapidly detect the status of the lines between two devices. When BFD detection is enabled between two adjacent RIP devices, if there is a line failure between the devices, BFD can quickly detect the failure and notify the RIP protocol. RIP will delete the RIP routes associated on the BFD interface. If these routes have backups, they will switch to the backup route in a very short time (affected by the BFD configuration). Currently, RIP supports BFD single-hop bidirectional detection only.

Table 19 Configuring RIP to Coordinate with BFD

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the RIP configuration mode	<b>router rip</b>	Mandatory  By default, RIP process is disabled.
Make all the interfaces covered by RIP process enable BFD function	<b>bfd all-interfaces</b>	Mandatory  By default, the BFD function of the interfaces covered by RIP is disabled.
Return to the global configuration mode	<b>exit</b>	-

Step	Command	Description
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Enable the BFD function on the interface	<b>ip rip bfd</b>	Mandatory By default, the BFD function of interface is disabled.

### Note

- For the BFD-related configurations, please see the Reliability Technology - BFD Technical Manual.

## 53.2.7 RIP monitoring and maintaining

Table 20 Configuring RIP Monitoring and Maintaining

Command	Description
<b>show ip rip</b> [ <i>vrf vrf-name</i> ]	Show the basic information of RIP
<b>show ip rip</b> [ <i>vrf vrf-name</i> ] <b>database</b> [ <b>detail</b>   <i>prefix/mask</i> [ [ <b>detail</b>   <b>longer-prefixes</b> [ <b>detail</b> ] ] ] ]	Show the RIP routing database information
<b>show ip rip</b> [ <i>vrf vrf-name</i> ] <b>statistics</b>	Show the statistical information of RIP
<b>show ip rip interface</b> [ <i>interface-name</i> ]	Show the RIP interface information
<b>clear ip rip</b> [ <i>vrf vrf-name</i> ] { <b>process</b>   <b>statistics</b> }	Clear the RIP process and statistical information

## 53.3 RIP typical configuration example

### 53.3.1 Configure RIP version

#### Network Requirements

- Run RIPv2 between Device1 and Device2 for route interaction.

#### Network Topology

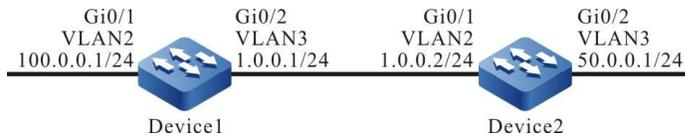


Figure 53 Network Topology for Configuring RIP Version

#### Configuration Steps

Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configure IP addresses for the ports. (Omitted)

Step 3: Configure RIP.

#### #Configure Device1.

```
Device1#configure terminal
Device1(config)#router rip
Device1(config-rip)#network 1.0.0.0
Device1(config-rip)#network 100.0.0.0
Device1(config-rip)#exit
```

#### #Configure Device2.

```
Device2#configure terminal
Device2(config)#router rip
Device2(config-rip)#network 1.0.0.0
Device2(config-rip)#network 50.0.0.0
Device2(config-rip)#exit
```

#### #View the routing table of Device1.

```
Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 1.0.0.0/24 is directly connected, 00:23:06, vlan3
R 50.0.0.0/8 [120/1] via 1.0.0.2, 00:13:26, vlan3
C 100.0.0.0/24 is directly connected, 00:23:06, vlan2
C 127.0.0.0/8 is directly connected, 76:51:00, lo0
```

#### #View the routing table of Device 2.

```
Device2#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
```

```

U - Per-user Static route
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 1.0.0.0/24 is directly connected, 00:23:06, vlan2
C 50.0.0/24 is directly connected, 00:23:06, vlan3
R 100.0.0.0/8 [120/1] via 1.0.0.1, 00:13:26, vlan2
C 127.0.0.0/8 is directly connected, 76:51:00, lo0

```

According to the routing table, the routing information advertised by the device uses 8-bit natural mask.

Step 4: Configure RIP version.

#Configure Device1.

```

Device1(config)#router rip
Device1(config-rip)#version 2
Device1(config-rip)#exit

```

#Configure Device2.

```

Device2(config)#router rip
Device2(config-rip)#version 2
Device2(config-rip)#exit

```

Step 5: Check the result.

#View the routing table of Device1.

```

Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
U - Per-user Static route
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 1.0.0.0/24 is directly connected, 00:23:06, vlan3
R 50.0.0.0/24 [120/1] via 1.0.0.2, 00:13:26, vlan3
C 100.0.0.0/24 is directly connected, 00:23:06, vlan2
C 127.0.0.0/8 is directly connected, 76:51:00, lo0

```

#View the routing table of Device 2.

```

Device2#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
U - Per-user Static route
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 1.0.0.0/24 is directly connected, 00:23:06, vlan2
C 50.0.0/24 is directly connected, 00:23:06, vlan3
R 100.0.0.0/24 [120/1] via 1.0.0.1, 00:13:26, vlan2
C 127.0.0.0/8 is directly connected, 76:51:00, lo0

```

According to the routing table, the routing information advertised by the device uses 24-bit accurate mask.

### 53.3.2 Configure RIP Route Redistribution

#### Network Requirements

- Run the OSPF protocol between Device1 and Device2. Device2 learns the OSPF routes 100.0.0.0/24 and 200.0.0.0/24 distributed by Device1.

- Run the RIPv2 protocol between Device2 and Device3. Device2 only redistributes the OSPF route 100.0.0.0/24 into RIP, and advertises such route to Device3.

### Network Topology

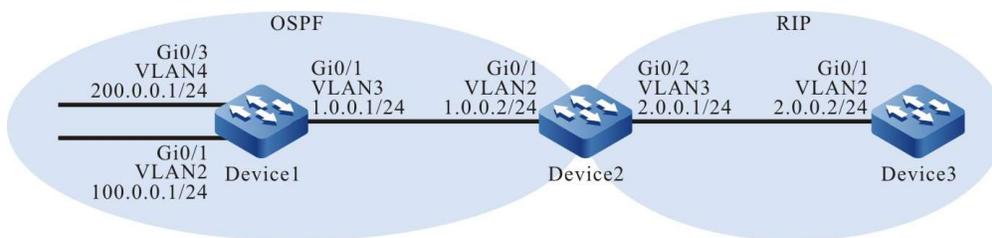


Figure 1 Network Topology for Configuring RIP Route Redistribution

### Configuration Steps

Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configure IP addresses for the ports. (Omitted)

Step 3: Configure OSPF.

#### #Configure Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#network 1.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 100.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 200.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#exit
```

#### #Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 1.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#exit
```

#### #View the routing table of Device 2.

```
Device2#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 1.0.0.0/24 is directly connected, 00:23:06, vlan2
C 2.0.0.0/24 is directly connected, 00:13:06, vlan3
O 100.0.0.0/24 [110/2] via 1.0.0.1, 00:04:12, vlan2
C 127.0.0.0/8 is directly connected, 76:51:00, lo0
O 200.0.0.0/24 [110/2] via 1.0.0.1, 00:04:12, vlan2
```

According to the routing table, Device2 learns the OSPF route advertised by Device1.

Step 4: Configure RIP.

#### #Configure Device2.

```
Device2(config)#router rip
Device2(config-rip)#version 2
```

```
Device2(config-rip)#network 2.0.0.0
Device2(config-rip)#exit
```

### #Configure Device3.

```
Device3#configure terminal
Device3(config)#router rip
Device3(config-rip)#version 2
Device3(config-rip)#network 2.0.0.0
Device3(config-rip)#exit
```

### Step 5: Configure routing policy.

#### #On Device2, configure route-map to invoke ACL to match 100.0.0.0/24 and filter 200.0.0.0/24.

```
Device2(config)#ip access-list standard 1
Device2(config-std-nacl)#permit 100.0.0.0 0.0.0.255
Device2(config-std-nacl)#commit
Device2(config-std-nacl)#exit
Device2(config)#route-map OSPFtoRIP
Device2(config-route-map)#match ip address 1
Device2(config-route-map)#exit
```

---

## Note

- When configuring a routing policy, both the prefix list and ACL can create filtering rules. The difference is that the prefix list can exactly match the routing mask.
- 

### Step 6: Configure RIP to redistribute OSPF routes.

#### #Configure Device2.

```
Device2(config)#router rip
Device2(config-rip)#redistribute ospf 100 route-map OSPFtoRIP
Device2(config-rip)#exit
```

### Step 7: Check the result.

#### #View the RIP routing table of Device 2.

```
Device2#show ip rip database
Types: N - Network, L - Learn, R - Redistribute, D - Default config, S - Static config
Proto: C - connected, S - static, R - RIP, O - OSPF, E - IRMP,
       o - SNSP, B - BGP, i-ISIS

RIP routing database in VRF kernel (Counter 3):
T/P Network      ProID Metric Next-Hop   From      Time Tag  Interface
N/C 2.0.0.0/24   none 1    --      --      0    vlan3
R/O 100.0.0.0/24  1    1    1.0.0.1 --      --      0    vlan2
```

#### #Check the routing table of Device3.

```

Device3#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 2.0.0.0/24 is directly connected, 00:23:06, vlan2
R 100.0.0.0/24 [120/1] via 2.0.0.1, 00:13:26, vlan2
C 127.0.0.0/8 is directly connected, 76:51:00, lo0

```

After checking the RIP routing tables of Device2 and Device3, you will find that the route 100.0.0.0/24 on Device2 has been redistributed to RIP and successfully advertised to Device3, while the route 200.0.0.0/24 has been successfully filtered.

---

## ⚠ Caution

- In practical applications, if the autonomous system has 2 or more edge routers, directly redistributing routes between different routing protocols is not recommended. When configuration is necessary, routing control policies such as filtering and summarization are required on the edge routers of the autonomous system to avoid routing loops.
- 

### 53.3.3 Configure the RIP Metric Offset

#### Network Requirements

- Run RIPv2 between Device1, Device2, Device3 and Device4 for interaction.
- Device1 learns the route 200.0.0.0/24 from both Device2 and Device3 at the same time.
- It is required to configure the routing metric offset in the receiving direction on Device1 to make Device1 first select the route advertised by Device2.

#### Network Topology

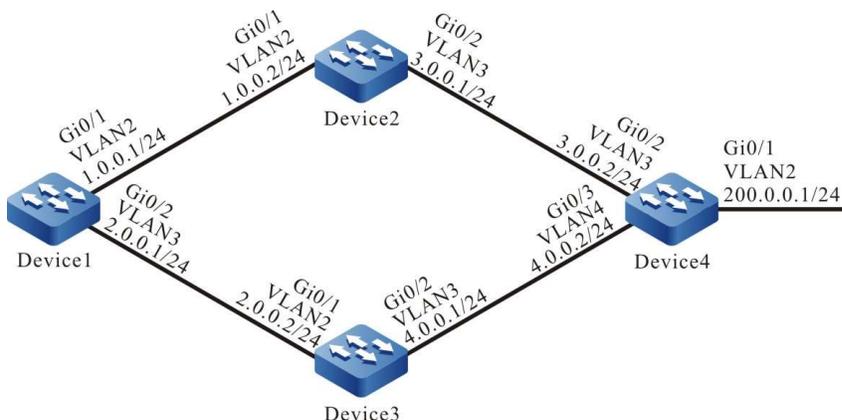


Figure 2 Network Topology for Configuring RIP Metric Offset

#### Configuration Steps

Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configure IP addresses for the ports. (Omitted)

Step 3: Configure RIP.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#router rip
Device1(config-rip)#version 2
Device1(config-rip)#network 1.0.0.0
Device1(config-rip)#network 2.0.0.0
Device1(config-rip)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#router rip
Device2(config-rip)#version 2
Device2(config-rip)#network 1.0.0.0
Device2(config-rip)#network 3.0.0.0
Device2(config-rip)#exit
```

#Configure Device3.

```
Device3#configure terminal
Device3(config)#router rip
Device3(config-rip)#version 2
Device3(config-rip)#network 2.0.0.0
Device3(config-rip)#network 4.0.0.0
Device3(config-rip)#exit
```

#Configure Device4.

```
Device4#configure terminal
Device4(config)#router rip
Device4(config-rip)#version 2
Device4(config-rip)#network 3.0.0.0
Device4(config-rip)#network 4.0.0.0
Device4(config-rip)#network 200.0.0.0
Device4(config-rip)#exit
```

#View the routing table of Device1.

```
Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 1.0.0.0/24 is directly connected, 00:23:06, vlan2
C 2.0.0.0/24 is directly connected, 00:22:56, vlan3
R 3.0.0.0/24 [120/1] via 1.0.0.2, 00:13:26, vlan2
R 4.0.0.0/24 [120/1] via 2.0.0.2, 00:11:04, vlan3
C 127.0.0.0/8 is directly connected, 76:51:00, lo0
R 200.0.0.0/24 [120/2] via 1.0.0.2, 00:08:31, vlan2
   [120/2] via 2.0.0.2, 00:08:31, vlan3
```

According to the routing table of Device1, there are two routes leading to 200.0.0.0/24.

Step 4: Configure access lists.

#Configure Device1.

```
Device1(config)#ip access-list standard 1
Device1(config-std-nacl)#permit 200.0.0.0 0.0.0.255
Device1(config-std-nacl)#commit
Device1(config-std-nacl)#exit
```

Step 5: Configure metric offset.

#Configure offset list on Device1 to increase the metric value of the route which is learned from interface VLAN3 and matches ACL by 3.

```
Device1(config)#router rip
Device1(config-rip)#offset-list 1 in 3 vlan3
Device1(config-rip)#exit
```

Step 6: Check the result.

#View the routing table of Device1.

```
Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 1.0.0.0/24 is directly connected, 00:33:59, vlan2
C 2.0.0.0/24 is directly connected, 00:33:50, vlan3
R 3.0.0.0/24 [120/1] via 1.0.0.2, 00:24:20, vlan2
R 4.0.0.0/24 [120/1] via 2.0.0.2, 00:21:57, vlan3
C 127.0.0.0/8 is directly connected, 77:01:54, lo0
R 200.0.0.0/24 [120/2] via 1.0.0.2, 00:19:25, vlan2
```

According to the routing table of Device1, the next hop output interface of route 200.0.0.0/24 is only VLAN2, which means that Device1 selects the route advertised by Device2.



- The route offset list can be used on all interfaces or specified interfaces, and in the receiving or advertising direction of the device.
- 

### 53.3.4 Configure RIP Route Filtration

#### Network Requirements

- Run RIPv2 between Device1 and Device2 for route interaction.
- The two routes 2.0.0.0/24 and 3.0.0.0/24 that are advertised by Device2 are learned on Device1, and then the latter route is filtered in the advertising direction of Device2.

## Network Topology

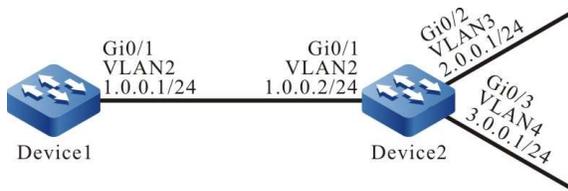


Figure 3 Network Topology for Configuring RIP Route Filtration

## Configuration Steps

Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configure IP addresses for the ports. (Omitted)

Step 3: Configure RIP.

### #Configure Device1.

```
Device1#configure terminal
Device1(config)#router rip
Device1(config-rip)#version 2
Device1(config-rip)#network 1.0.0.0
Device1(config-rip)#exit
```

### #Configure Device2.

```
Device2#configure terminal
Device2(config)#router rip
Device2(config-rip)#version 2
Device2(config-rip)#network 1.0.0.0
Device2(config-rip)#network 2.0.0.0
Device2(config-rip)#network 3.0.0.0
Device2(config-rip)#exit
```

### #View the routing table of Device1.

```
Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 1.0.0.0/24 is directly connected, 00:23:06, vlan2
R 2.0.0.0/24 [120/1] via 1.0.0.2, 00:13:26, vlan2
R 3.0.0.0/24 [120/1] via 1.0.0.2, 00:13:26, vlan2
C 127.0.0.0/8 is directly connected, 76:51:00, lo0
```

According to the result, Device1 learns two routes distributed by Device2.

Step 4: Configure access lists.

### #Configure Device2.

```
Device2(config)#ip access-list standard 1
Device2(config-std-nacl)#permit 2.0.0.0 0.0.0.255
Device2(config-std-nacl)#commit
Device2(config-std-nacl)#exit
```

---

## Note

- When configuring route filtration, both the prefix list and ACL can create filtering rules. The difference is that the prefix list can exactly match the routing mask.
- 

Step 5: Configure route filtration.

#Configure route filtration in the outgoing direction of the interface VLAN2 of Device2.

```
Device2(config)#router rip
Device2(config-rip)#distribute-list 1 out vlan2
Device2(config-rip)#exit
```

Step 6: Check the result.

#View the routing information of Device1.

```
Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 1.0.0.0/24 is directly connected, 00:23:06, vlan2
R 2.0.0.0/24 [120/1] via 1.0.0.2, 00:13:26, vlan2
C 127.0.0.0/8 is directly connected, 76:51:00, lo0
```

According to the result, Device2 will not advertise the route 3.0.0.0/24 to Device1. It is cleared from the routing table of Device1 only after timeout of the route.

---

## Note

- The distribute-list can be used on all interfaces or specified interfaces, and in the receiving or advertising direction of the device.
- 

### 53.3.5 Configure RIP Route Summarization

#### Network Requirements

- Run RIPv2 between Device1, Device2, Device3 and Device4 for route interaction.
- Device1 learns two routes, i.e. 100.1.0.0/24 and 100.2.0.0/24, from Device2. In order to reduce the size of the routing table of Device1, Device2 needs to distribute the summarized route of these two routes only to Device1.

## Network Topology

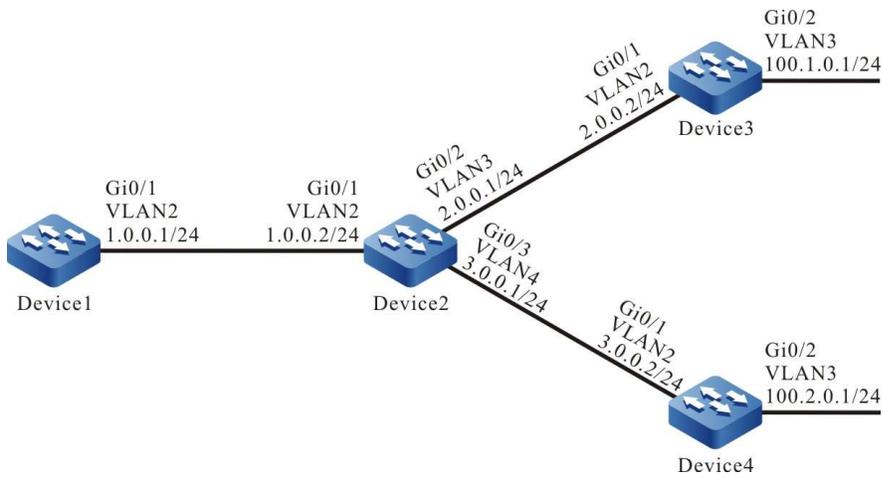


Figure 4 Network Topology for Configuring RIP Route Summarization

### Configuration Steps

Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configure IP addresses for the ports. (Omitted)

Step 3: Configure RIP.

#### #Configure Device1.

```
Device1#configure terminal
Device1(config)#router rip
Device1(config-rip)#version 2
Device1(config-rip)#network 1.0.0.0
Device1(config-rip)#exit
```

#### #Configure Device2.

```
Device2#configure terminal
Device2(config)#router rip
Device2(config-rip)#version 2
Device2(config-rip)#network 1.0.0.0
Device2(config-rip)#network 2.0.0.0
Device2(config-rip)#network 3.0.0.0
Device2(config-rip)#exit
```

#### #Configure Device3.

```
Device3#configure terminal
Device3(config)#router rip
Device3(config-rip)#version 2
Device3(config-rip)#network 2.0.0.0
Device3(config-rip)#network 100.0.0.0
Device3(config-rip)#exit
```

#### #Configure Device4.

```
Device4#configure terminal
Device4(config)#router rip
Device4(config-rip)#version 2
Device4(config-rip)#network 3.0.0.0
Device4(config-rip)#network 100.0.0.0
```

```
Device4(config-rip)#exit
```

#View the routing table of Device1.

```
Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 1.0.0.0/24 is directly connected, 00:23:06, vlan2
R 2.0.0.0/24 [120/1] via 1.0.0.2, 00:13:26, vlan2
R 3.0.0.0/24 [120/1] via 1.0.0.2, 00:13:26, vlan2
R 100.1.0.0/24 [120/2] via 1.0.0.2, 00:08:31, vlan2
R 100.2.0.0/24 [120/2] via 1.0.0.2, 00:08:31, vlan2
C 127.0.0.0/8 is directly connected, 76:51:00, lo0
```

Step 4: Configure interface route summarization.

#Configure the summarized route 100.0.0.0/8 on Device2.

```
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ip summary-address rip 100.0.0.0/8
Device2(config-if-vlan2)#exit
```

Step 5: Check the result.

#View the routing table of Device1.

```
Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 1.0.0.0/24 is directly connected, 00:24:06, vlan2
R 2.0.0.0/24 [120/1] via 1.0.0.2, 00:14:26, vlan2
R 3.0.0.0/24 [120/1] via 1.0.0.2, 00:14:26, vlan2
R 100.0.0.0/8 [120/2] via 1.0.0.2, 00:00:31, vlan2
C 127.0.0.0/8 is directly connected, 76:51:00, lo0
```

According to the result, Device1 learns the summarized route 100.0.0.0/8 distributed by Device2. The two detail routes are cleared from the routing table only after time out.

---

## Note

- RIP supports global automatic summarization and manual interface summarization. The global automatic summarization of RIPv2 is disabled by default.
-

### 53.3.6 Configure RIP to Coordinate with BFD

#### Network Requirements

- Run RIPv2 between Device1, Device2 and Device3 for route interaction.
- Device1 learns the route 3.0.0.0/24 from both Device2 and Device3. By configuring route offset, it makes Device1 first select the route advertised by Device2. Then, the route from Device1 to Device2 is its main line; the route from Device1 to Device3 is its backup line.
- Configure BFD between Device1 and Device2. When the line between Device1 and Device2 fails, configure RIP to associate with BFD between Device1 and Device2 to quickly detect the line failure. When BFD identifies the main line failure, it will trigger RIP for route update, and the route 3.0.0.0/24 will be switched to the backup line.

#### Network Topology

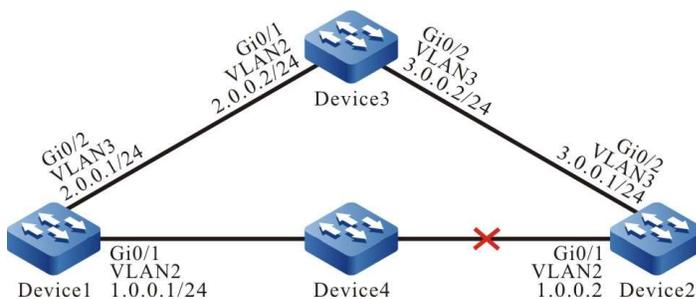


Figure 5 Network Topology for Configuring Coordination of RIP with BFD

#### Configuration Steps

Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configure IP addresses for the ports. (Omitted)

Step 3: Configure RIP.

#### #Configure Device1.

```
Device1#configure terminal
Device1(config)#router rip
Device1(config-rip)#version 2
Device1(config-rip)#network 1.0.0.0
Device1(config-rip)#network 2.0.0.0
Device1(config-rip)#exit
```

#### #Configure Device2.

```
Device2#configure terminal
Device2(config)#router rip
Device2(config-rip)#version 2
Device2(config-rip)#network 1.0.0.0
Device2(config-rip)#network 3.0.0.0
Device2(config-rip)#exit
```

### #Configure Device3.

```
Device3#configure terminal
Device3(config)#router rip
Device3(config-rip)#version 2
Device3(config-rip)#network 2.0.0.0
Device3(config-rip)#network 3.0.0.0
Device3(config-rip)#exit
```

### #View the routing table of Device1.

```
Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 1.0.0.0/24 is directly connected, 01:30:23, vlan2
C 2.0.0.0/24 is directly connected, 01:30:14, vlan3
R 3.0.0.0/24 [120/1] via 1.0.0.2, 01:20:44, vlan2
   [120/1] via 2.0.0.2, 00:00:02, vlan3
C 127.0.0.0/8 is directly connected, 77:58:18, lo0
```

According to the result, Device1 learns the route 3.0.0.0/24 from both Device2 and Device3 at the same time.

### Step 4: Configure route offset.

#Configure offset list in the incoming direction of interface VLAN3 on Device1 to increase the metric value of the route which matches ACL by 3.

```
Device1(config)#ip access-list standard 1
Device1(config-std-nacl)#permit 3.0.0.0 0.0.0.255
Device1(config-std-nacl)#commit
Device1(config)#exit
Device1(config)#router rip
Device1(config-rip)#offset-list 1 in 3 vlan3
Device1(config-rip)#exit
```

### #View the routing table of Device1.

```
Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 1.0.0.0/24 is directly connected, 01:30:23, vlan2
C 2.0.0.0/24 is directly connected, 01:30:14, vlan3
R 3.0.0.0/24 [120/1] via 1.0.0.2, 01:20:44, vlan2
C 127.0.0.0/8 is directly connected, 77:58:18, lo0
```

According to the result, after configuring route offset, Device1 selects the route 3.0.0.0/24 advertised by Device2.

### Step 5: Configure BFD.

### #Configure Device1.

```
Device1(config)#bfd fast-detect
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ip rip bfd
Device1(config-if-vlan2)#exit
```

### #Configure Device2.

```

Device2(config)#bfd fast-detect
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ip rip bfd
Device2(config-if-vlan2)#exit

```

Step 6: Check the result.

#View the BFD information on Device1.

```

Device1#show bfd session
OurAddr      NeighAddr      LD/RD      State      Holddown      interface
1.0.0.1      1.0.0.2        2/4        UP         5000          vlan2

```

#When the lines between Device1 and Device2 fail, the route can quickly switch to the backup line.

#View the routing information on Device1.

```

Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 2.0.0.0/24 is directly connected, 02:07:47, vlan3
R 3.0.0.0/24 [120/4] via 2.0.0.2, 00:01:14, vlan3
C 127.0.0.0/8 is directly connected, 78:35:51, lo0

```

### 53.3.7 Configure an RIP Standby Interface

#### Network Requirements

- Run RIPv2 between Device1, Device2 and Device3 for route interaction.
- Device1 learns the route 3.0.0.0/24 from both Device2 and Device3. By configuring route offset, it makes Device1 first select the route advertised by Device2. Then, the line between Device1 and Device2 is its main line; the line between Device1 and Device3 is its backup line.
- Configure RIP backup interface on Device1. When the main line is normal, if the main line through which the route passes fails, the route can quickly switch to the backup line.

#### Network Topology

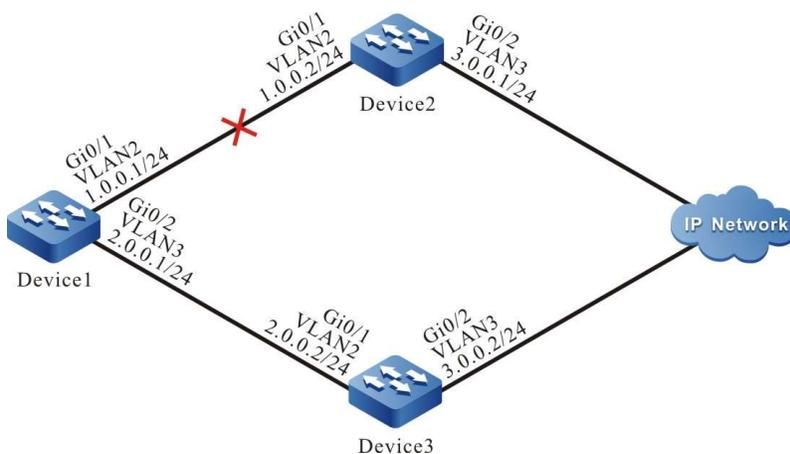


Figure 6 Network Topology for Configuring RIP Backup Interface

### Configuration Steps

Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configure IP addresses for the ports. (Omitted)

Step 3: Configure RIP.

#### #Configure Device1.

```
Device1#configure terminal
Device1(config)#router rip
Device1(config-rip)#version 2
Device1(config-rip)#network 1.0.0.0
Device1(config-rip)#network 2.0.0.0
Device1(config-rip)#exit
```

#### #Configure Device2.

```
Device2#configure terminal
Device2(config)#router rip
Device2(config-rip)#version 2
Device2(config-rip)#network 1.0.0.0
Device2(config-rip)#network 3.0.0.0
Device2(config-rip)#exit
```

#### #Configure Device3.

```
Device3#configure terminal
Device3(config)#router rip
Device3(config-rip)#version 2
Device3(config-rip)#network 2.0.0.0
Device3(config-rip)#network 3.0.0.0
Device3(config-rip)#exit
```

#### #View the routing table of Device1.

```
Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 1.0.0.0/24 is directly connected, 01:30:23, vlan2
C 2.0.0.0/24 is directly connected, 01:30:14, vlan3
R 3.0.0.0/24 [120/1] via 1.0.0.2, 01:20:44, vlan2
               [120/1] via 2.0.0.2, 00:00:02, vlan3
C 127.0.0.0/8 is directly connected, 77:58:18, lo0
```

According to the result, Device1 learns the route 3.0.0.0/24 from both Device2 and Device3 at the same time.

Step 4: Configure route offset.

#Configure offset list in the incoming direction of interface VLAN3 on Device1 to increase the metric value of the route which matches ACL by 3.

```
Device1(config)#ip access-list standard 1
Device1(config-std-nacl)#permit 3.0.0.0 0.0.0.255
Device1(config-std-nacl)#commit
```

```
Device1(config)#exit
Device1(config)#router rip
Device1(config-rip)#offset-list 1 in 3 vlan3
Device1(config-rip)#exit
```

#View the routing table of Device1.

```
Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 1.0.0.0/24 is directly connected, 01:30:23, vlan2
C 2.0.0.0/24 is directly connected, 01:30:14, vlan3
R 3.0.0.0/24 [120/1] via 1.0.0.2, 01:20:44, vlan2
C 127.0.0.0/8 is directly connected, 77:58:18, lo0
```

According to the result, after configuring route offset, Device1 selects the route 3.0.0.0/24 advertised by Device2.

Step 5: Configure backup interface.

#On Device1, configure the interface VLAN3 as the RIP backup interface of VLAN2.

```
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ip rip standby vlan3
Device1(config-if-vlan2)#exit
```

Step 6: Check the result.

#When the lines between Device1 and Device2 fail, the route can quickly switch to the backup line between Device1 and Device3.

#View the routing information on Device1.

```
Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 2.0.0.0/24 is directly connected, 02:07:47, vlan3
R 3.0.0.0/24 [120/4] via 2.0.0.2, 00:01:14, vlan3
C 127.0.0.0/8 is directly connected, 78:35:51, lo0
```

## 53.3.8 Configure a Passive RIP Interface

### Network Requirements

- Run RIPv2 between Device1 and Device2 for route interaction.
- Configure passive interface on Device1 so that it doesn't send update packets to Device2.

### Network Topology

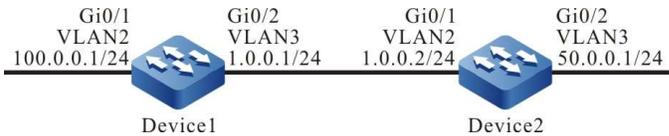


Figure 7 Network Topology for Configuring Passive RIP Interface

### Configuration Steps

Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configure IP addresses for the ports. (Omitted)

Step 3: Configure RIP.

#### #Configure Device1.

```
Device1#configure terminal
Device1(config)#router rip
Device1(config-rip)#version 2
Device1(config-rip)#network 1.0.0.0
Device1(config-rip)#network 100.0.0.0
Device1(config-rip)#exit
```

#### #Configure Device2.

```
Device2#configure terminal
Device2(config)#router rip
Device2(config-rip)#version 2
Device2(config-rip)#network 1.0.0.0
Device2(config-rip)#network 50.0.0.0
Device2(config-rip)#exit
```

#### #View the routing table of Device1.

```
Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 1.0.0.0/24 is directly connected, 00:23:06, vlan3
R 50.0.0.0/24 [120/1] via 1.0.0.2, 00:13:26, vlan3
C 100.0.0.0/24 is directly connected, 00:23:06, vlan2
C 127.0.0.0/8 is directly connected, 76:51:00, lo0
```

#### #View the routing table of Device 2.

```
Device2#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 1.0.0.0/24 is directly connected, 00:23:06, vlan2
C 50.0.0.0/24 is directly connected, 00:23:06, vlan3
R 100.0.0.0/24 [120/1] via 1.0.0.1, 00:13:26, vlan2
C 127.0.0.0/8 is directly connected, 76:51:00, lo0
```

Step 4: Configure a passive interface.

#Configure Device1.

```
Device1(config)#router rip
Device1(config-rip)#passive-interface vlan3
Device1(config-rip)#exit
```

Configure VLAN3 as a passive interface on Device1 so that it doesn't send update packets to Device2, though it can still receive such packets.

Step 5: Check the result.

#View the routing table of Device1.

```
Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 1.0.0.0/24 is directly connected, 00:23:06, vlan3
R 50.0.0.0/24 [120/1] via 1.0.0.2, 00:13:26, vlan3
C 100.0.0.0/24 is directly connected, 00:23:06, vlan2
C 127.0.0.0/8 is directly connected, 76:51:00, lo0
```

The routing information of 50.0.0.0/24 will still be saved on Device1. For Device2, the routing information of 100.0.0.0/24 will be removed from the routing table after the RIP route is deleted for time out.

#View the routing table of Device 2.

```
Device2#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 1.0.0.0/24 is directly connected, 00:25:06, vlan2
C 50.0.0.0/24 is directly connected, 00:25:06, vlan3
C 127.0.0.0/8 is directly connected, 77:51:00, lo0
```

# 54 RIPng

---

## 54.1 Overview

RIPng, also known as the next generation of RIP protocol (RIP next generation), is a dynamic routing protocol used in IPv6 networks to provide routing information for IPv6 packet forwarding. RIPng is the result of extending RIP-2. Its working principle almost the same as RIP. In order to adapt to the IPv6 network, RIPng is different from the original RIP in the following aspects:

- UDP port number: RIPng uses the port number 521 of UDP to send and receive protocol packets;
- Multicast address: RIPng protocol uses FF02::9 as the multicast address of the RIPng router within the local scope of the link. It does not support broadcast;
- Prefix length: The RIPng protocol routing destination address has a 128-bit prefix length;
- Next hop address: RIPng uses a 128-bit IPv6 address;
- Source address: RIPng uses the local address FE80::/10 of the link as the source address to send RIPng packets.

The RIPng-related protocol specifications include RFC2080 and RFC2081.

## 54.2 RIPng function configuration

Table 54 RIPng Function Configuration List

Configuration Task	
Configure RIPng Basic Functions	Globally Enable RIPng
Configure RIPng Route Generation	Configure RIPng to Distribute Default Route
	Configure RIPng Route Redistribution
Configure RIPng Route Control	Configure the RIPng Administrative Distance
	Configure RIPng Route Summarization
	Configure RIPng Metric Offset
	Configure RIPng Route Filtration
	Configure Metric Value of RIPng Interface
	Configure the Routing Flag for an RIPng Interface
	Configure the Maximum Load Balancing of RIPng
Configure RIPng Network Optimization	Configure RIPng Timers
	Configure Split Horizon and Toxicity Reverse of RIPng
	Configure a Static RIPng Neighbor
	Configure Passive RIPng Interface

## 54.2.1 Configure RIPng Basic Functions

### Configuration Condition

Before configuring the basic functions of RIPng, ensure that:

- The link layer protocol has been configured to ensure normal communication at the link layer.
- Enable the IPv6 capability of the interface.

### Globally Enable RIPng

To use RIPng, the following configurations are required:

- Create RIPng process;
- Configure the interface to enable RIPng.

Table 54-2 Globally Enabling RIPng

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Create RIPng process and enter RIPng configuration mode	<b>ipv6 router rip</b> <i>process-id</i>	Mandatory By default, RIPng process is disabled.
Return to global configuration mode	<b>exit</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Globally enable RIPng for the interface	<b>ipv6 rip enable</b> <i>process-id</i>	Mandatory By default, RIPng is disabled on the interface.

## 54.2.2 Configure RIPng Route Generation

### Configuration Condition

Before configuring RIPng route generation, ensure that:

- Enable the IPv6 capability of the interface;
- Enable RIPng.

## Configure RIPng to Distribute Default Route

Through configuration, the device sends default routes under all RIPng interfaces and sets itself as the default gateway of other adjacent devices.

Table 541 Configuring RIPng to Distribute Default Route

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter RIPng configuration mode	<b>ipv6 router rip <i>process-id</i></b>	Mandatory By default, RIPng process is disabled.
Configure RIPng to Distribute Default Route	<b>default-information originate [ <i>metric value</i> ]</b>	Mandatory By default, RIPng doesn't distribute default route.

---

### Note

- If a default route (0::/0) is learned, it will replace the default route (::/0) distributed by the device. When there is loop in the network, route oscillation may be caused. Thus, when using this command, be sure that several other devices in the same routing domain are not enabling it at the same time.
- 

## Configure RIPng Route Redistribution

The routes generated by other protocols can be imported into RIPng by configuring route redistribution.

Table 54-2 Configuring RIPng Route Redistribution

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter RIPng configuration mode	<b>ipv6 router rip <i>process-id</i></b>	Mandatory By default, RIPng process is disabled.

Step	Command	Description
Configure the default metric value of importing other routing protocol by RIPng	<b>default-metric</b> <i>metric-value</i>	Optional By default, the default metric value of importing other routing protocol is 1.
Configure RIPng Route Redistribution	<b>redistribute</b> <i>protocol</i> [ <i>protocol-id</i> ] [ <b>metric</b> <i>metric-value</i> ] [ <b>route-map</b> <i>route-map-name</i> ] [ <b>match</b> <i>route-sub-type</i> ]	Mandatory By default, no route redistribution is configured.

### Note

- In case of redistribution, after the metric command option is specified, the route redistributed will adopt this metric value.
- For RIPng, when configuring route redistribution application routing map, the match options supported include ipv6 address, route type, tag, interface, ipv6 nexthop, ipv6 route-source and metric, and the set options supported include metric and tag.

## 54.2.3 Configure RIPng Route Control

### Configuration Condition

Before configuring RIPng route control, ensure that:

- Enable the IPv6 capability of the interface;
- Enable RIPng.

### Configure the RIPng Administrative Distance

Multiple routing protocols can run in the device at the same time. The device selects the routes learned by each protocol through administrative distance. The smaller the administrative distance, the more like the route is selected.

Table 54-3 Configuring RIPng Administrative Distance

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Enter RIPng configuration mode	<b>ipv6 router rip</b> <i>process-id</i>	-
Configure the RIPng Administrative Distance	<b>distance</b> <i>distance-value</i>	Mandatory By default, RIPng administrative distance is 120.

### Configure RIPng Route Summarization

RIPng route summarization means to configure a pair of destination address and mask combination, which will summarize the routes in the covered network segment.

After RIPng route summarization is configured, the device only advertises the summarized routes. This can significantly reduce the scale of adjacent RIPng routing tables in large and medium-sized networks and the consumption of network bandwidth by routing protocol packets.

The metric of the summarized route will be the minimum metric value among all subnet routes.

Table 54-4 Configuring RIPng Route Summarization Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure the route summarization function of RIPng on the interface	<b>ipv6 rip summary-address</b> <i>prefix-address</i>	Mandatory By default, no route summarization function is configured.

### Configure RIPng Metric Offset

By default, RIPng applies the route metric advertised by the neighbor device to the received routes. To modify the metric in some special application scenarios, you can configure the RIPng metric offset to correct the metric of the specified route.

If the metric in the incoming direction is configured, RIPng modifies the metric of the received routes and saves the routes into the routing table. When RIP advertises a metric to the neighbor devices, it uses the

new metric. If the metric in the outgoing direction is configured, the metric is modified only when RIP advertises a metric to the neighbor devices.

Table 54-5 Configuring RIPng Matrix Offset

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter RIPng configuration mode	<b>ipv6 router rip</b> <i>process-id</i>	Mandatory By default, RIPng process is disabled.
Configure RIPng to modify the metric of the specified route	<b>offset-list</b> <i>access-list-name</i> { <b>in</b>   <b>out</b> } <i>metric-offset</i> [ <i>interface-name</i> ]	Mandatory By default, no metric value of interface is configured.

### Configure RIPng Route Filtration

A router can filter the received or advertised routes by configuring an Access Control List (ACL), prefix list or routing map. In receiving RIPng routes, you can filter some learnt routes; or in advertising RIPng routes, you can filter some routes that are advertised to neighbor devices.

Table 54-6 Configuring RIPng Route Filtration

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter RIPng configuration mode	<b>ipv6 router rip</b> <i>process-id</i>	Mandatory By default, RIPng process is disabled.
Configure RIPng route filtration function	<b>distribute-list</b> { <i>access-list-name</i>   <b>prefix</b> <i>prefix-list-name</i>   <b>route-map</b> <i>route-map-name</i> } { <b>in</b>   <b>out</b> } [ <i>interface-name</i> ]	Mandatory By default, no route filtration function is configured. When the route filtration function is configured, if an interface is not specified, route filtration will be enabled for all RIPng interfaces.

### Configure Metric Value of RIPng Interface

After RIPng is enabled for an interface, the corresponding direct route is generated in the database, with the default metric being 1. When the route is in the RIPng database or it is advertised to neighbor devices, if the interface is configured with a metric, the interface metric is used as the metric of the route.

If the interface metric is changed, the RIPng database immediately updates the corresponding direct route of RIPng and advertises the new metric to the neighbor devices.

Table 54-7 Configuring RIPng Interface Matrix

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure RIPng interface metric	<b>ipv6 rip metric</b> <i>metric-value</i>	Mandatory By default, the matrix value of the RIPng interface is 1.

### Note

- When the matrix value of the RIPng interface is configured, the matrix of the direct subnet on the interface instead of that of route learning will be affected.

### Configure the Routing Flag for an RIPng Interface

The network administrator can attach tags to some routes. Then, in applying a routing policy, the network administrator can perform route filtration or route property advertisement based on the tags.

Table 54-8 Configuring RIPng Interface Routing Tag

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-

Step	Command	Description
Configure the routing tag on the direct subnet on the interface of RIPng	<b>ipv6 rip tag tag-value</b>	Mandatory By default, no routing tag is configured.

### Configure the maximum number of load balancing entries of RIPng

This command helps you to control the number of RIPng load balancing entries for routing.

Table 54-11 Configuring Maximum Number of Load Balancing Entries of RIPng

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter RIPng configuration mode	<b>ipv6 router rip process-id</b>	Mandatory By default, RIPng process is disabled.
Configure the maximum number of load balancing entries of RIPng	<b>maximum-paths max-number</b>	Optional By default, the maximum number of load balancing entries of RIPng is 4.

## 54.2.4 Configure RIPng Network Optimization

### Configuration Condition

Before configuring RIPng network optimization, ensure that:

- Enable the IPv6 capability of the interface;
- Enable RIPng.

### Configure RIPng Timers

RIPng does not maintain neighbor relations and it does not support route withdrawn; therefore, the protocol provides four configurable timers to control the network convergence speed. The four timers are: route update timer, route timeout timer, route dampening update timer, and route clear timer.

The route timeout time must be at least three times of the route update time. If no route update packet is received within the route timeout time, the route becomes invalid and it enters a dampening cycle. The length of the dampening cycle is determined by the dampening update time. During the cycle, the route

will not be cleared. After the dampening cycle is completed, the route enters the clear cycle. During the cycle, the route can be updated. However, if no route update packet is received during the cycle, the route will be deleted.

Table 54-12 Configuring RIPng Timer

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter RIPng configuration mode	<b>ipv6 router rip <i>process-id</i></b>	Mandatory By default, RIPng process is disabled.
Configure the time of RIPng timer	<b>timers <i>update-interval</i> <i>invalid-interval</i> <i>holddown-interval</i> <i>flush-interval</i></b>	Optional By default, the RIPng update interval is 30 seconds, the effective time of advertisement 180 seconds, the suppression time 0 seconds, and the clearing time 120 seconds.

---

 **Caution**

- In the same RIPng routing domain, the **timer** configurations on all devices must be consistent to avoid network flapping.
- 

### Configure Split Horizon and Toxicity Reverse of RIPng

Split horizon and toxicity reverse are mechanisms that are used to prevent route loops.

1. Configure split horizon.

RIPng does not advertise routes that it has learnt from an interface to the interface, preventing routing loops.

Table 54-13 Configuring RIPng Split Horizon

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure RIPng split horizon	<b>no ipv6 split-horizon</b> [ <b>disable</b> ]	Optional By default, the split horizon function is enabled.

## 2. Configure toxicity reverse.

RIPng announces routes that have been learnt from an interface to the interface, but the route metric is the maximum number of hops, 16, preventing routing loops.

Table 54-14 Configuring RIPng Toxicity Reverse

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure RIPng toxicity reverse	<b>ipv6 split-horizon poison-reverse</b>	Mandatory By default, the toxicity reverse function is disabled.

### Note

- The split horizon and toxicity reverse functions are valid only for the learnt routes, direct routes on the RIPng, and the redistributed direct and static routes.
- The split horizon function and the toxicity reversion function cannot be used at the same time.

## Configure a Static RIPng Neighbor

RIPng does not maintain neighbor relations, so it does not have the concept of neighbor. Here the neighbor refers to the neighbor RIPng routing device. After a static RIPng neighbor is specified, RIPng sends RIPng packets to the neighbor in unicast mode. The configuration is applied to a network that does not support broadcast or multicast, such as point-to-point links. If the configuration is applied to a multicast network, it may cause repeated RIPng packets in the network.

Table 54-15 Configuring Static RIPng Neighbor

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure the neighbor which advertises routing information in the form of unicast	<b>ipv6 rip neighbor</b> <i>ipv6-address</i>	Mandatory The parameter <i>ipv6-address</i> is the ipv6 address of the direct interface on the peer port.

### Note

- The advertisement of routing information to static neighbors occurs only on the RIPng interface, and "**pv6 rip passive**" cannot prevent them from sending packets to static neighbors.

### Configure Passive RIPng Interface

To decrease the network bandwidth consumed by the routing protocol, the dynamic routing protocol uses the passive interface function. RIPng receives only route update packets on a passive interface, and it does not send route update packets on the passive interface. In a low-speed network with small bandwidth, the passive interface function and the neighbor function cooperate to effectively reduce interactions of RIPng routes.

Table 54-16 Configuring Passive RIPng Interface

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure Passive RIPng Interface	<b>ipv6 rip passive</b>	Mandatory By default, no passive interface is configured.

### Note

- The **ipv6 rip passive** function does not restrain an interface from sending unicast route updates to its neighbor devices. When the passive interface function is used with the **neighbor** command, the function does not restrain an interface from sending unicast route updates to its neighbor devices. This application mode controls a router so that it sends route updates only to some neighbor devices in unicast mode instead of sending route updates to all neighbor devices in multicast mode.

## 54.2.5 Configure RIPng to Coordinate with BFD

The backup interface can be used in specific application environments only. It cannot meet the requirements of real-time backup. The BFD (Bidirectional Forwarding Detection) function of RIPng which provides end-to-end protection can achieve rapid route convergence and switch. BFD can rapidly detect the status of the lines between two devices. When BFD detection is enabled between two adjacent RIPng devices, if there is a line failure between the devices, BFD can quickly detect the failure and notify the RIPng protocol. RIP will delete the RIPng routes associated on the BFD interface. If these routes have backups, they will switch to the backup route in a very short time (affected by the BFD configuration). Currently, RIPng supports BFD single-hop bidirectional detection only.

Table 54-17 Configuring RIPng to Coordinate with BFD

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter RIPng configuration mode	<b>ipv6 router rip 100</b>	Mandatory By default, RIPng process is disabled.

Step	Command	Description
Make all the interfaces covered by RIPng process enable BFD function	<b>bfd all-interfaces</b>	Mandatory By default, the BFD function of all interfaces covered by RIPng is disabled.
Return to the global configuration mode	<b>exit</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Enable the BFD function on the interface	<b>ipv6 rip bfd</b>	Mandatory By default, the BFD function of interface is disabled.

### Note

- For the BFD-related configurations, please see the Reliability Technology - BFD Technical Manual.

## 54.2.6 PIM-DM monitoring and maintaining

Table 54-18 Configuring RIPng Monitoring and Maintaining

Command	Description
<b>clear ipv6 rip</b> [ <i>process-id</i> ] { <b>process</b>   <b>statistics</b> }	Clear the RIPng process and statistical information
<b>show ipv6 rip</b> [ <i>process-id</i> ]	Show the basic information of RIPng
<b>show ipv6 rip</b> [ <i>process-id</i> ] <b>database</b> [ <b>detail</b>   <i>ipv6-address/mask-length</i> [ <b>detail</b>   <b>longer-prefixes</b> ] ]	Show the RIPng routing database information
<b>show ipv6 rip</b> [ <i>process-id</i> ] <b>statistics</b> [ <i>interface-name</i> ]	Show the statistical information of RIPng interface

Command	Description
<b>show ipv6 rip interface</b> [ <i>interface-name</i> ]	Show RIPng interface information

## 54.3 RIPng Typical Configuration Example

### 54.3.1 Configure RIPng Basic Functions

#### Network Requirements

- Run RIPng between Device1 and Device2 for route interaction.

#### Network Topology

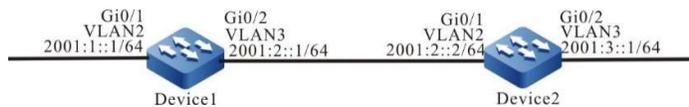


Figure 54 Network Topology for Configuring Basic Functions of RIPng

#### Configuration Steps

Step 1: Configure VLAN, and add ports to the required VLAN. (Omitted)

Step 2: Configure IPv6 addresses for the ports. (Omitted)

Step 3: Configure RIPng.

#### #Configure Device1.

```
Device1#configure terminal
Device1(config)#ipv6 router rip 100
Device1(config-ripng)#exit
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#ipv6 rip enable 100
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan 3
Device1(config-if-vlan3)#ipv6 rip enable 100
Device1(config-if-vlan3)#exit
```

#### #Configure Device2.

```
Device2#configure terminal
Device2(config)#ipv6 router rip 100
Device2(config-ripng)#exit
Device2(config)#interface vlan 2
Device2(config-if-vlan2)#ipv6 rip enable 100
Device2(config-if-vlan2)#exit
Device2(config)#interface vlan 3
Device2(config-if-vlan3)#ipv6 rip enable 100
Device2(config-if-vlan3)#exit
```

Step 4: Check the result.

#View the IPv6 routing table of Device1.

```
Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
  via ::, 2w4d:19:31:05, lo0
C 2001:1::/64 [0/0]
  via ::, 00:21:42, vlan2
L 2001:1::1/128 [0/0]
  via ::, 00:21:40, lo0
C 2001:2::/64 [0/0]
  via ::, 00:21:34, vlan3
L 2001:2::1/128 [0/0]
  via ::, 00:21:33, lo0
R 2001:3::/64 [120/2]
  via fe80::201:7aff:fec3:38a4, 00:11:19, vlan3
```

#View the IPv6 routing table of Device 2.

```
Device2#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
  via ::, 3d:22:39:31, lo0
R 2001:1::/64 [120/2]
  via fe80::201:7aff:fe01:204, 00:12:00, vlan2
C 2001:2::/64 [0/0]
  via ::, 00:30:46, vlan2
L 2001:2::2/128 [0/0]
  via ::, 00:30:45, lo0
C 2001:3::/64 [0/0]
  via ::, 00:29:12, vlan3
L 2001:3::1/128 [0/0]
  via ::, 00:29:11, lo0
```

According to the routing table, the routing information advertised by the device uses 64-bit accurate mask.

## 54.3.2 Configure RIPng Route Redistribution

### Network Requirements

- Run the IPv6 OSPF protocol between Device1 and Device2. Device2 learns the IPv6 OSPF routes 2001:1::/64 and 2001:2::/64 distributed by Device1.
- Run the RIPng protocol between Device2 and Device3. Device2 only redistributes the IPv6 OSPF route 2001:1::/64 into RIPng, and advertises such route to Device3.

### Network Topology

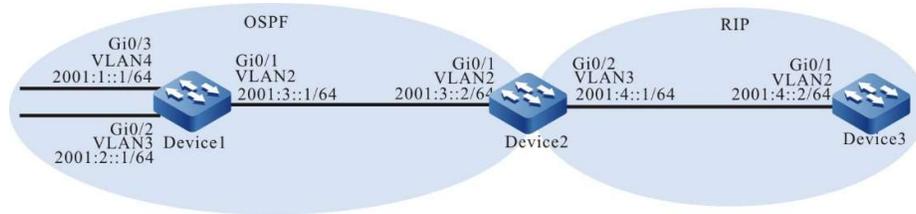


Figure 54 Network Topology for Configuring RIPng Route Redistribution

### Configuration Steps

Step 1: Configure VLAN, and add ports to the required VLAN. (Omitted)

Step 2: Configure IPv6 addresses for the ports. (Omitted)

Step 3: Configure IPv6 OSPF.

#### #Configure Device1.

```
Device1#configure terminal
Device1(config)#ipv6 router ospf 100
Device1(config-ospf6)# router-id 1.1.1.1
Device1(config-ospf6)#exit
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#ipv6 router ospf tag 100 area 0
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan 3
Device1(config-if-vlan3)#ipv6 router ospf tag 100 area 0
Device1(config-if-vlan3)#exit
Device1(config)#interface vlan 4
Device1(config-if-vlan4)#ipv6 router ospf tag 100 area 0
Device1(config-if-vlan4)#exit
```

#### #Configure Device2.

```
Device2#configure terminal
Device2(config)#ipv6 router ospf 100
Device2(config-ospf6)#router-id 2.2.2.2
Device2(config-ospf6)#exit
Device2(config)#interface vlan 2
Device2(config-if-vlan2)#ipv6 router ospf tag 100 area 0
Device2(config-if-vlan2)#exit
```

#### #View the IPv6 routing table of Device 2.

```
Device2#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
  via ::, 4d:00:09:49, lo0
O 2001:1::/64 [110/2]
  via fe80::201:7aff:fe01:204, 00:12:16, vlan2
O 2001:2::/64 [110/2]
  via fe80::201:7aff:fe01:204, 00:12:16, vlan2
C 2001:3::/64 [0/0]
  via ::, 00:19:51, vlan2
L 2001:3::2/128 [0/0]
  via ::, 00:19:50, lo0
C 2001:4::/64 [0/0]
  via ::, 00:45:13, vlan3
L 2001:4::1/128 [0/0]
```

```
via ::, 00:45:12, lo0
```

According to the routing table, Device2 learns the IPv6 OSPF route advertised by Device1.

Step 4: Configure RIPng.

#Configure Device2.

```
Device2(config)#ipv6 router rip 100
Device2(config-ripng)#exit
Device2(config)#interface vlan 3
Device2(config-if-vlan3)#ipv6 rip enable 100
Device2(config-if-vlan3)#exit
```

#Configure Device3.

```
Device3#configure terminal
Device3(config)#ipv6 router rip 100
Device3(config-ripng)#exit
Device3(config)#interface vlan 2
Device3(config-if-vlan2)#ipv6 rip enable 100
Device3(config-if-vlan2)#exit
```

Step 5: Configure routing policy.

#On Device2, configure route-map to invoke the prefix list to match 2001:1::/64 and filter 2001:2::/64.

```
Device2(config)#ipv6 prefix-list OSPF permit 2001:1::/64
Device2(config)#route-map OSPFtoRIP
Device2(config-route-map)#match ipv6 address prefix-list OSPF
Device2(config-route-map)#exit
```

---

### Note

- When configuring a routing policy, both the prefix list and ACL can create filtering rules. The difference is that the prefix list can exactly match the routing mask.
- 

Step 6: Configure RIPng redistribution of IPv6 OSPF route.

#Configure RIPng redistribution of IPv6 OSPF route.

```
Device2(config)#ipv6 router rip 100
Device2(config-ripng)#redistribute ospf 100 route-map OSPFtoRIP
Device2(config-ripng)#exit
```

Step 7: Check the result.

#View the RIPng database on Device2.

```
Device2#show ipv6 rip database
Type : N - Network interface, L - Learn, R - Redistribute, D - Default config,
      S - Static config
Proto: C - connected, S - static, R - RIP, O - OSPF, E - IRMP,
      o - SNSP, B - BGP, i-ISIS

RIPng process 100 routing database (VRF Kernel, Counter 2):
[Type/Proto]
[R/O] 2001:1::/64 metric 1
```

```
via vlan2, fe80::201:7aff:fe01:204, no expires
[N/C] 2001:4::/64 metric 1, installed
via vlan3, ::, no expires
```

### # Check the IPv6 routing table of Device3.

```
Device3#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
U - Per-user Static route
O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
via ::, 2w0d:20:00:11, lo0
R 2001:1::/64 [120/2]
via fe80::201:7aff:fec3:38a5, 02:50:14, vlan2
C 2001:4::/64 [0/0]
via ::, 03:56:24, vlan2
L 2001:4::2/128 [0/0]
via ::, 03:56:23, lo0
```

After checking the database of Device2 and routing table of Device3, you will find that the route 2001:1::/64 on Device2 has been redistributed to RIPng and successfully advertised to Device3, while the route 2001:2::/64 has been successfully filtered.

---

### Note

- In practical applications, if the autonomous system has 2 or more edge routers, directly redistributing routes between different routing protocols is not recommended. When configuration is necessary, routing control policies such as filtering and summarization are required on the edge routers of the autonomous system to avoid routing loops.
- 

## 54.3.3 Configure RIPng Metric Offset

### Network Requirements

- Run RIPng between Device1, Device2, Device3 and Device4 for interaction.
- Device1 learns the route 2001:5::/64 from both Device2 and Device3 at the same time.
- It is required to configure the routing metric offset in the receiving direction on Device1 to make Device1 first select the route advertised by Device2.

### Network Topology

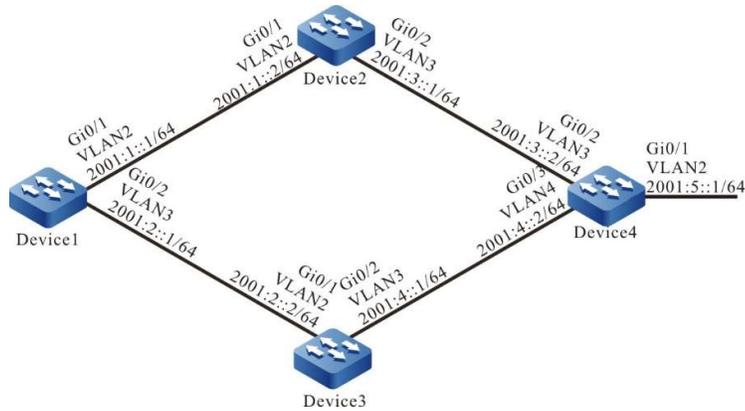


Figure 54 Network Topology for Configuring RIPng Metric Offset

### Configuration Steps

- Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)
- Step 2: Configure IPv6 addresses for the ports. (Omitted)
- Step 3: Configure RIPng.

#### #Configure Device1.

```
Device1#configure terminal
Device1(config)#ipv6 router rip 100
Device1(config-ripng)#exit
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#ipv6 rip enable 100
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan 3
Device1(config-if-vlan3)#ipv6 rip enable 100
Device1(config-if-vlan3)#exit
```

#### #Configure Device2.

```
Device2#configure terminal
Device2(config)#ipv6 router rip 100
Device2(config-ripng)#exit
Device2(config)#interface vlan 2
Device2(config-if-vlan2)#ipv6 rip enable 100
Device2(config-if-vlan2)#exit
Device2(config)#interface vlan 3
Device2(config-if-vlan3)#ipv6 rip enable 100
Device2(config-if-vlan3)#exit
```

#### #Configure Device3.

```
Device3#configure terminal
Device3(config)#ipv6 router rip 100
Device3(config-ripng)#exit
Device3(config)#interface vlan 2
Device3(config-if-vlan2)#ipv6 rip enable 100
Device3(config-if-vlan2)#exit
Device3(config)#interface vlan 3
Device3(config-if-vlan3)#ipv6 rip enable 100
Device3(config-if-vlan3)#exit
```

#### #Configure Device4.

```

Device4#configure terminal
Device4(config)#ipv6 router rip 100
Device4(config-ripng)#exit
Device4(config)#interface vlan 2
Device4(config-if-vlan2)#ipv6 rip enable 100
Device4(config-if-vlan2)#exit
Device4(config)#interface vlan 3
Device4(config-if-vlan3)#ipv6 rip enable 100
Device4(config-if-vlan3)#exit
Device4(config)#interface vlan 4
Device4(config-if-vlan4)#ipv6 rip enable 100
Device4(config-if-vlan4)#exit

```

#View the IPv6 routing table of Device1.

```

Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
  via ::, 2w5d:06:21:24, lo0
C 2001:1::/64 [0/0]
  via ::, 00:02:05, vlan2
L 2001:1::1/128 [0/0]
  via ::, 00:02:04, lo0
C 2001:2::/64 [0/0]
  via ::, 00:02:02, vlan3
L 2001:2::1/128 [0/0]
  via ::, 00:02:01, lo0
R 2001:3::/64 [120/2]
  via fe80::201:7aff:fec3:38a4, 00:02:03, vlan2
R 2001:4::/64 [120/2]
  via fe80::201:7aff:fe11:2214, 00:00:48, vlan3
R 2001:5::/64 [120/3]
  via fe80::201:7aff:fec3:38a4, 00:02:03, vlan2
  [120/3]
  via fe80::201:7aff:fe11:2214, 00:00:48, vlan3

```

According to the routing table of Device1, there are two routes leading to 2001:5::/64.

Step 4: Configure access lists.

```

Device1(config)#ipv6 access-list extended RIPng
Device1(config-v6-list)#permit 10 2001:5::/64 any
Device1(config-v6-list)#commit
Device1(config-v6-list)#exit

```

Step 5: Configure metric offset.

#Configure offset list on Device1 to increase the metric value of the route which is learned from interface VLAN3 and matches ACL by 3.

```

Device1(config)# ipv6 router rip 100
Device1(config-ripng)#offset-list RIPng in 3 vlan 3
Device1(config-ripng)#exit

```

Step 6: Check the result.

#View the IPv6 routing table of Device1.

```

Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]

```

```

via ::, 2w5d:06:34:28, lo0
C 2001:1::/64 [0/0]
via ::, 00:15:09, vlan2
L 2001:1::1/128 [0/0]
via ::, 00:15:08, lo0
C 2001:2::/64 [0/0]
via ::, 00:15:06, vlan3
L 2001:2::1/128 [0/0]
via ::, 00:15:05, lo0
R 2001:3::/64 [120/2]
via fe80::201:7aff:fec3:38a4, 00:03:10, vlan2
R 2001:4::/64 [120/2]
via fe80::201:7aff:fe11:2214, 00:03:10, vlan3
R 2001:5::/64 [120/3]
via fe80::201:7aff:fec3:38a4, 00:03:10, vlan2

```

According to the routing table of Device1, the next hop output interface of route 2001:5::/64 is only VLAN2, which means that Device1 selects the route advertised by Device2.

---

### Note

- The route offset list can be used on all interfaces or specified interfaces, and in the receiving or advertising direction of the device.
- 

## 54.3.4 Configure RIPng Route Filtration

### Network Requirements

- Run RIPng between Device1 and Device2 for route interaction.
- The two routes 2001:2::/64 and 2001:3::/64 that are advertised by Device2 are learned on Device1, and then the latter route is filtered in the advertising direction of Device2.

### Network Topology

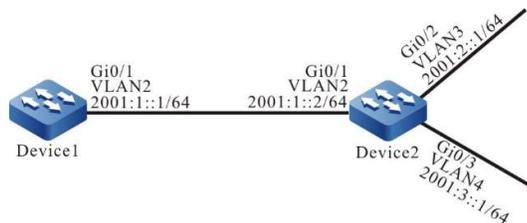


Figure 54 Network Topology for Configuring RIPng Route Filtration

### Configuration Steps

- Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)
- Step 2: Configure IPv6 addresses for the ports. (Omitted)
- Step 3: Configure RIPng.

## #Configure Device1.

```
Device1#configure terminal
Device1(config)#ipv6 router rip 100
Device1(config-ripng)#exit
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#ipv6 rip enable 100
Device1(config-if-vlan2)#exit
```

## #Configure Device2.

```
Device2#configure terminal
Device2(config)#ipv6 router rip 100
Device2(config-ripng)#exit
Device2(config)#interface vlan 2
Device2(config-if-vlan2)#ipv6 rip enable 100
Device2(config-if-vlan2)#exit
Device2(config)#interface vlan 3
Device2(config-if-vlan3)#ipv6 rip enable 100
Device2(config-if-vlan3)#exit
Device2(config)#interface vlan 4
Device2(config-if-vlan4)#ipv6 rip enable 100
Device2(config-if-vlan4)#exit
```

## #View the IPv6 routing table of Device1.

```
Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
  via ::, 2w5d:02:47:44, lo0
C 2001:1::/64 [0/0]
  via ::, 00:56:34, vlan2
L 2001:1::1/128 [0/0]
  via ::, 00:56:32, lo0
R 2001:2::/64 [120/2]
  via fe80::201:7aff:fec3:38a4, 00:27:11, vlan2
R 2001:3::/64 [120/2]
  via fe80::201:7aff:fec3:38a4, 00:27:11, vlan2
```

According to the result, Device1 learns two routes distributed by Device2.

### Step 4: Configure IPv6 prefix list.

```
Device2(config)#ipv6 prefix-list RIPng deny 2001:3::/64
```

### Step 5: Configure route filtration.

## #Configure route filtration in the outgoing direction of the interface VLAN2 of Device2.

```
Device2(config)#ipv6 router rip 100
Device2(config-ripng)#distribute-list prefix RIPng out vlan 2
Device2(config-ripng)#exit
```

### Step 6: Check the result.

## #View the IPv6 routing table of Device1.

```
Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
  via ::, 2w5d:03:03:49, lo0
```

```

C 2001:1::/64 [0/0]
  via ::, 01:12:39, vlan2
L 2001:1::1/128 [0/0]
  via ::, 01:12:38, lo0
R 2001:2::/64 [120/2]
  via fe80::201:7aff:fec3:38a4, 00:43:16, vlan2

```

According to the result, Device2 will not advertise the route 2001:3::/64 to Device1. It is cleared from the routing table of Device1 only after timeout of the route.

## Note

- The distribute-list can be used on all interfaces or specified interfaces, and in the receiving or advertising direction of the device.

### 54.3.5 Configure RIPng Route Summarization

#### Network Requirements

- Run RIPng between Device1, Device2, Device3 and Device4 for route interaction.
- Device1 learns two routes, i.e. 2001:4:1:1::/64 and 2001:4:1:2::/64, from Device2. In order to reduce the size of the routing table of Device1, Device2 needs to distribute the summarized route of these two routes only to Device1.

#### Network Topology

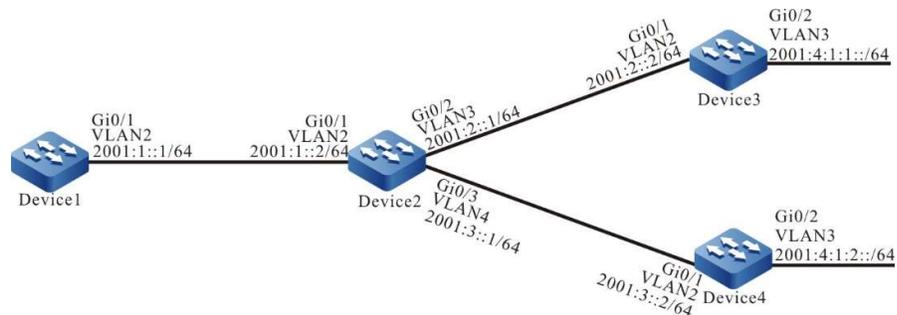


Figure 1 Network Topology for Configuring RIPng Route Summarization

#### Configuration Steps

- Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)
- Step 2: Configure IPv6 addresses for the ports. (Omitted)
- Step 3: Configure RIPng.

#### #Configure Device1.

```

Device1#configure terminal
Device1(config)#ipv6 router rip 100
Device1(config-ripng)#exit
Device1(config)#interface vlan 2

```

```
Device1(config-if-vlan2)#ipv6 rip enable 100
Device1(config-if-vlan2)#exit
```

#### #Configure Device2.

```
Device2#configure terminal
Device2(config)#ipv6 router rip 100
Device2(config-ripng)#exit
Device2(config)#interface vlan 2
Device2(config-if-vlan2)#ipv6 rip enable 100
Device2(config-if-vlan2)#exit
Device2(config)#interface vlan 3
Device2(config-if-vlan3)#ipv6 rip enable 100
Device2(config-if-vlan3)#exit
Device2(config)#interface vlan 4
Device2(config-if-vlan4)#ipv6 rip enable 100
Device2(config-if-vlan4)#exit
```

#### #Configure Device3.

```
Device3#configure terminal
Device3(config)#ipv6 router rip 100
Device3(config-ripng)#exit
Device3(config)#interface vlan 2
Device3(config-if-vlan2)#ipv6 rip enable 100
Device3(config-if-vlan2)#exit
Device3(config)#interface vlan 3
Device3(config-if-vlan3)#ipv6 rip enable 100
Device3(config-if-vlan3)#exit
```

#### #Configure Device4.

```
Device4#configure terminal
Device4(config)#ipv6 router rip 100
Device4(config-ripng)#exit
Device4(config)#interface vlan 2
Device4(config-if-vlan2)#ipv6 rip enable 100
Device4(config-if-vlan2)#exit
Device4(config)#interface vlan 3
Device4(config-if-vlan3)#ipv6 rip enable 100
Device4(config-if-vlan3)#exit
```

#### #View the IPv6 routing table of Device1.

```
Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
  via ::, 2w5d:02:27:40, lo0
C 2001:1::/64 [0/0]
  via ::, 00:36:29, vlan2
L 2001:1::1/128 [0/0]
  via ::, 00:36:28, lo0
R 2001:2::/64 [120/2]
  via fe80::201:7aff:fec3:38a4, 00:07:06, vlan2
R 2001:3::/64 [120/2]
  via fe80::201:7aff:fec3:38a4, 00:07:06, vlan2
R 2001:4:1:1::/64 [120/3]
  via fe80::201:7aff:fec3:38a4, 00:07:06, vlan2
R 2001:4:1:2::/64 [120/3]
  via fe80::201:7aff:fec3:38a4, 00:06:55, vlan2
```

Step 4: Configure interface route summarization.

#### #Configure the summarized route 2001:4:1::/48 on Device2.

```
Device2(config)#interface vlan 2
```

```
Device2(config-if-vlan2)#ipv6 rip summary-address 2001:4:1::/48
Device2(config-if-vlan2)#exit
```

Step 5: Check the result.

#View the IPv6 routing table of Device1.

```
Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
  via ::, 2w5d:02:35:44, lo0
C 2001:1::/64 [0/0]
  via ::, 00:44:33, vlan2
L 2001:1::1/128 [0/0]
  via ::, 00:44:32, lo0
R 2001:2::/64 [120/2]
  via fe80::201:7aff:fec3:38a4, 00:15:10, vlan2
R 2001:3::/64 [120/2]
  via fe80::201:7aff:fec3:38a4, 00:15:10, vlan2
R 2001:4:1::/48 [120/3]
  via fe80::201:7aff:fec3:38a4, 00:05:19, vlan2
```

According to the result, Device1 learns the summarized route 2001:4:1::/48 distributed by Device2. The two detail routes are cleared from the routing table only after time out.

### 54.3.6 Configure Passive RIPng Interface

#### Network Requirements

- Run RIPng between Device1 and Device2 for route interaction.
- Configure passive interface on Device1 so that it doesn't send update packets to Device2.

#### Network Topology

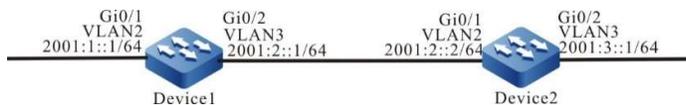


Figure 2 Network Topology for Configuring Passive RIPng Interface

#### Configuration Steps

- Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)
- Step 2: Configure IPv6 addresses for the ports. (Omitted)
- Step 3: Configure RIPng.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#ipv6 router rip 100
Device1(config-ripng)#exit
Device1(config)#interface vlan 2
```

```
Device1(config-if-vlan2)#ipv6 rip enable 100
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan 3
Device1(config-if-vlan3)#ipv6 rip enable 100
Device1(config-if-vlan3)#exit
```

#### #Configure Device2.

```
Device2#configure terminal
Device2(config)#ipv6 router rip 100
Device2(config-ripng)#exit
Device2(config)#interface vlan 2
Device2(config-if-vlan2)#ipv6 rip enable 100
Device2(config-if-vlan2)#exit
Device2(config)#interface vlan 3
Device2(config-if-vlan3)#ipv6 rip enable 100
Device2(config-if-vlan3)#exit
```

#### #View the IPv6 routing table of Device1.

```
Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
  via ::, 2w4d:19:31:05, lo0
C 2001:1::/64 [0/0]
  via ::, 00:21:42, vlan2
L 2001:1::1/128 [0/0]
  via ::, 00:21:40, lo0
C 2001:2::/64 [0/0]
  via ::, 00:21:34, vlan3
L 2001:2::1/128 [0/0]
  via ::, 00:21:33, lo0
R 2001:3::/64 [120/2]
  via fe80::201:7aff:fec3:38a4, 00:11:19, vlan3
```

#### #View the IPv6 routing table of Device 2.

```
Device2#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
  via ::, 3d:22:39:31, lo0
R 2001:1::/64 [120/2]
  via fe80::201:7aff:fe01:204, 00:12:00, vlan2
C 2001:2::/64 [0/0]
  via ::, 00:30:46, vlan2
L 2001:2::2/128 [0/0]
  via ::, 00:30:45, lo0
C 2001:3::/64 [0/0]
  via ::, 00:29:12, vlan3
L 2001:3::1/128 [0/0]
  via ::, 00:29:11, lo0
```

#### Step 4: Configure a passive interface.

#### #Configure Device1.

```
Device1(config)#interface vlan 3
Device1(config-if-vlan3)#ipv6 rip passive
Device1(config-if-vlan3)#exit
```

Configure vlan 3 as a passive interface on Device1 so that it doesn't send update packets to Device2, though it can still receive such packets.

Step 5: Check the result.

#View the IPv6 routing table of Device1.

```
Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
  via ::, 2w4d:19:55:37, lo0
C 2001:1::/64 [0/0]
  via ::, 00:46:14, vlan2
L 2001:1::1/128 [0/0]
  via ::, 00:46:12, lo0
C 2001:2::/64 [0/0]
  via ::, 00:46:06, vlan3
L 2001:2::1/128 [0/0]
  via ::, 00:46:05, lo0
R 2001:3::/64 [120/2]
  via fe80::201:7aff:fec3:38a4, 00:35:51, vlan3
```

The routing information of 2001:3::/64 will still be saved on Device1. For Device2, the routing information of 2001:1::/64 will be removed from the routing table after the RIPng route is deleted for time out.

#View the IPv6 routing table of Device 2.

```
Device2#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
  via ::, 3d:23:05:24, lo0
C 2001:2::/64 [0/0]
  via ::, 00:56:39, vlan2
L 2001:2::2/128 [0/0]
  via ::, 00:56:38, lo0
C 2001:3::/64 [0/0]
  via ::, 00:55:05, vlan3
L 2001:3::1/128 [0/0]
  via ::, 00:55:04, lo0
```

### 54.3.7 Configure RIPng to use IPSec encryption & authentication

#### Network Requirements

- Run RIPng between Device1 and Device2.
- Device1 and Device2 use IPSec tunnels for encryption & authentication of RIPng packets.
- Upon completion of the configuration, the device can normally conduct route interaction.

#### Network Topology

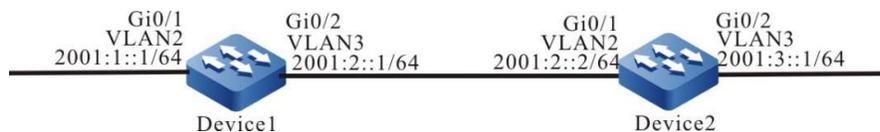


Figure 3 Network Topology for Configuring RIPng Authentication Function

### Configuration Steps

Step 1: Configure VLAN, and add ports to the required VLAN; configure the IPv6 address of each interface. (Omitted)

Step 2: Configure RIPng process and enable the RIPng function on the interface.

```
#Configure Device1.  
Device1#configure terminal  
Device1(config)#ipv6 router rip 100  
Device1(config-ripng)#exit  
Device1(config)#interface vlan2  
Device1(config-if-vlan2)#ipv6 rip enable 100  
Device1(config-if-vlan2)#exit  
Device1(config)#interface vlan3  
Device1(config-if-vlan3)#ipv6 rip enable 100  
Device1(config-if-vlan3)#exit
```

#Configure Device2.

```
Device2#configure terminal  
Device2(config)#ipv6 router rip 100  
Device2(config-ripng)#exit  
Device2(config)#interface vlan2  
Device2(config-if-vlan2)#ipv6 rip enable 100  
Device2(config-if-vlan2)#exit  
Device2(config)#interface vlan3  
Device2(config-if-vlan3)#ipv6 rip enable 100  
Device2(config-if-vlan3)#exit
```

Step 3: Configure IPsec proposal and manual tunnel.

#On Device1, create IPsec proposal a, use ESP transmission & encapsulation mode (encryption algorithm 3des, authentication algorithm sha1), create IPsec manual tunnel a, and configure SPI and key.

```
Device1(config)#crypto ipsec proposal a  
Device1(config-ipsec-prop)#mode transport  
Device1(config-ipsec-prop)#esp 3des sha1  
Device1(config-ipsec-prop)#exit  
Device1(config)#crypto ipv6-tunnel a manual  
Device1(config-manual-tunnel)#set ipsec proposal a  
Device1(config-manual-tunnel)#set inbound esp 1000 encryption 0 11111111111111111111111111111111 authentication 0 aaaaaaaaaa  
aaaaaaaaa  
Device1(config-manual-tunnel)#set outbound esp 1001 encryption 0 aaaaaaaaaaaaaaaaaaaaaaa authentication 0 111111111111  
11111111  
Device1(config-manual-tunnel)#exit
```

#On Device2, create IPsec proposal a, use ESP transmission & encapsulation mode (encryption algorithm 3des, authentication algorithm sha1), create IPsec manual tunnel a, and configure SPI and key.

```
Device2(config)#crypto ipsec proposal a  
Device2(config-ipsec-prop)#mode transport  
Device2(config-ipsec-prop)#esp 3des sha1  
Device2(config-ipsec-prop)#exit  
Device2(config)#crypto ipv6-tunnel a manual  
Device2(config-manual-tunnel)#set ipsec proposal a  
Device2(config-manual-tunnel)#set inbound esp 1001 encryption 0 aaaaaaaaaaaaaaaaaaaaaaa authentication 0 111111111111  
11111111  
Device2(config-manual-tunnel)#set outbound esp 1000 encryption 0 11111111111111111111111111111111 authentication 0 aaaaaaaaaa
```

```
aaaaaaaaa
Device2(config-manual-tunnel)#exit
```

Step 4: In the RIPng process, bind corresponding IPsec tunnel to each interface.

**#Bind IPsec tunnel a to the interface Vlan3 of Device1**

```
Device1(config)#interface vlan3
Device1(config-if-vlan3)#ipv6 rip ipsec-tunnel a
Device1(config-if-vlan3)#exit
```

**#Bind IPsec tunnel a to the interface Vlan2 of Device2**

```
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ipv6 rip ipsec-tunnel a
Device2(config-if-vlan2)#exit
```

Step 5: Check the result.

**#View the RIPng interface information of Vlan3 on Device1.**

```
Device1#show ipv6 rip interface vlan3
vlan3 is up, line protocol is up
RIPng enable status   : Enable on process 100
RIPng running status  : Up
VPN Routing/Forwarding : Kernel
Passive interface     : Disabled
Split horizon         : enable
Packet MTU            : 1500
Joined RIPng multicast : Yes
IPv6 interface address :
2001:2::1/64
fe80::201:7aff:fe74:55e7/10
RIPng bfd interface   : Enable
RIPng bfd function open : OFF
RIPng bfd interface state : DOWN
RIPng ipsec-tunnel info:
Bind to ipsec-tunnel :a
Tunnel-id: 0
```

**#View the IPv6 routing table of Device1.**

```
Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
via ::, 2w4d:19:31:05, lo0
C 2001:1::/64 [0/0]
via ::, 00:21:42, vlan2
L 2001:1::1/128 [0/0]
via ::, 00:21:40, vlan2
C 2001:2::/64 [0/0]
via ::, 00:21:34, vlan3
L 2001:2::1/128 [0/0]
via ::, 00:21:33, vlan3
R 2001:3::/64 [120/2]
via fe80::201:7aff:fec3:38a4, 00:11:19, vlan3
```

**#View the IPv6 routing table of Device 2.**

```
Device2#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
```

U - Per-user Static route  
O - OSPF, OE-OSPF External, M - Management

```
L ::1/128 [0/0]
  via ::, 3d:22:39:31, lo0
R 2001:1::/64 [120/2]
  via fe80::201:7aff:fe01:204, 00:12:00, vlan2
C 2001:2::/64 [0/0]
  via ::, 00:30:46, vlan2
L 2001:2::2/128 [0/0]
  via ::, 00:30:45, vlan2
C 2001:3::/64 [0/0]
  via ::, 00:29:12, vlan3
L 2001:3::1/128 [0/0]
  via ::, 00:29:11, vlan3
```

According to the routing table, the IPsec tunnel has been successfully bound, and the packets are sent and received normally so that the routes can be learnt from each other.

---

 说明:

- When configuring RIPng to bind an IPsec tunnel, you can configure process binding or interface binding only, or configure both process and interface binding.
  - When IPsec tunnel is configured for process binding and interface binding at the same time, the latter takes effect first.
-

# 55 OSPF

---

## 55.1 Overview

OSPF protocol (Open Shortest Path First) is a dynamic routing protocol based on link status. It uses Dijkstra's shortest path precedence algorithm SPF to calculate routes in a single autonomous system (Autonomous System, hereinafter referred to as AS).

The OSPF protocol, developed by IETF, is mainly used to solve problems like slow convergence and loop formation in distance vector routing. It can be applied in large and medium-sized networks. The OSPF version 2 currently implemented complies with RFC2328 and supports the OSPF extended functions defined by other related RFCs.

In OSPF protocol, each device maintains a link status database which describes the AS network. Devices in the same area have the same database. After the database is fully synchronized, each device deems itself as the root and uses the SPF algorithm to calculate a loop-free shortest path tree to describe the shortest path it knows to reach each destination. Finally, each device builds its own routing table according to the SPF tree.

OSPF has the following characteristics:

- Fast convergence: Send update packets immediately after the topological structure of the network changes, and synchronize this change in the AS;
- No self-loop: OSPF runs SPF to calculate routes based on the link status database, which ensures that no routing loops will be formed through the algorithm itself;
- Division of areas: OSPF allows the AS to be divided into multiple areas, which reduces the occupation of network bandwidth and makes it possible to build a hierarchical network;
- Support authentication: Every time the OSPF device receives a routing protocol packet, it will verify the authentication information in the packet to avoid information leakage or malicious attacks in the network;
- Support subnets of different lengths: The route advertised by OSPF carries network masks to support subnets of different lengths;
- Support load balancing: Support multiple equal-cost routes leading to the same

destination address.

## 55.2 OSPF function configuration

Table 1 OSPF Function Configuration List

Configuration Task	
Configure OSPF Basic Functions	Configure OSPF Protocol
Configure OSPF Area	Configure OSPF NSSA
	Configure OSPF Stub Area
	Configure OSPF Virtual Link
Configure OSPF Network Type	Configure Network Type of OSPF Interface as Broadcast
	Configure Network Type of OSPF Interface as P2P
	Configure Network Type of OSPF Interface as NBMA
	Configure Network Type of OSPF Interface as P2MP
Configure OSPF Network Authentication	Configure OSPF Area Authentication
	Configure OSPF Interface Authentication
Configure OSPF Route Generation	Configure OSPF Route Redistribution
	Configure OSPF Default Route
	Configure OSPF Host Route
Configure OSPF Route Control	Configure OSPF Inter-area Summarization
	Configure OSPF External Route Summarization
	Configure OSPF Inter-area Route Filtration
	Configure OSPF External Route Filtration
	Configure OSPF Route Installation Filtration

Configuration Task	
	Configure Cost Value of OSPF Interface
	Configure OSPF Reference Bandwidth
	Configure OSPF Administrative Distance
	Configure the Maximum Number of Load Balancing Entries of OSPF
	Configure OSPF to be Compatible with RFC1583
Configure OSPF Network Optimization	Configure Keepalive Time of OSPF Neighbors
	Configure Passive OSPF Interface
	Configure OSPF Demand Circuit
	Configure OSPF Interface Priority
	Configure OSPF Interface MTU
	Configure Transfer Delay of OSPF Interface
	Configure OSPF LSA Retransmission
	Configure OSPF to Prohibit LSA Diffusion
	Configure OSPF SPF Calculation Time
	Configure OSPF Database Overflow
Configure OSPF to Coordinate with BFD	Configure OSPF to Coordinate with BFD
Configure OSPF GR	Configure OSPF GR Restarter
	Configure OSPF GR Helper

## 55.2.1 Configure OSPF Basic Functions

In the various configuration tasks of OSPF, you must first enable the OSPF protocol so that the configuration of the other function features can take effect.

### Configuration Condition

Before configuring basic functions of OSPF, first complete the following tasks:

- The link layer protocol has been configured to ensure normal communication at the link layer.
- Interface IP addresses have been configured so that neighbor nodes are reachable at the network layer.

### Configure OSPF Protocol

To enable the OSPF function, you need to create an OSPF process first, specify the network address scope associated with this process and the area to which the address scope belongs; if an interface IP address is within the network segment of a certain area, the interface belongs to this area and enables the OSPF function, and OSPF will advertise the direct route of this interface.

The device where OSPF protocol is running must have a Router ID, which is used to uniquely identify a device in an OSPF AS. The uniqueness of the Router ID in the AS must be guaranteed. Otherwise, it will influence the neighbor establishment and route learning. A Router ID may be specified in the process of creating OSPF process. If no Router ID is specified, election will be conducted according to the following rules:

- Firstly, select the largest IP address from the Loopback interface as Router ID;
- If no Loopback interface is configured for IP address, select the largest IP addresses from other interfaces as Router ID;
- Only when the interface is UP can the interface address be selected as Router ID.

OSPF supports multiple processes that are identified with process number, and different processes are independent of each other.

Table 2 Enabling OSPF Procotol

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Create OSPF process and enter OSPF configuration mode	<b>router ospf</b> <i>process-id</i> [ <b>vrf</b> <i>vrf-name</i> ]	Mandatory Enable the OSPF process directly or from VRF. By

Step	Command	Description
		<p>default, the OSPF protocol is disabled in the system.</p> <p>When OSPF is enabled from VRF, the OSPF process belonging to a certain VRF can manage the interfaces belonging to this VRF only.</p>
Configure the network segment covered by OSPF area	<b>network</b> <i>ip-address wildcard-mask</i> <b>area</b> <i>area-id</i>	<p>Mandatory</p> <p>By default, interface doesn't belong to any OSPF process or area.</p> <p>One interface can only belong to one OSPF process and area.</p>
Configure Router ID of OSPF process	<b>router-id</b> <i>ip-address</i>	<p>Optional</p> <p>By default, it is generated according to the electing rules of Router ID.</p> <p>Modifying the Router ID will not cause the OSPF neighbors to become invalid. To enable the newly configured Router ID to take effect, manual resetting of the process is required.</p>

### 55.2.2 Configure OSPF Area

In order to reduce the CPU and memory usage by a large amount of database information, the OSPF AS is divided into multiple areas. The area is identified by a 32-bit area ID, which can be represented by a decimal number ranging from 0 to 4294967295 or an IP address within 0.0.0.0 - 255.255.255.255. Area 0 or 0.0.0.0 means the backbone area of OSPF, and others are non-backbone areas. All the inter-area routing information needs to be forwarded through backbone areas. Routing information cannot be directly exchanged between non-backbone areas.

OSPF defines several types of routers:

- Internal Router: The device whose all interfaces belong to the same area;

- Area Border Router (ABR): The device connecting to multiple areas;
- Autonomous System Boundary Router (ASBR): The device which imports external route for OSPF AS.

### Configuration Condition

Before configuring OSPF area, ensure that:

- Interface IP addresses have been configured so that neighbor nodes are reachable at the network layer;
- Enable OSPF protocol.

### Configure OSPF NSSA

Type-7 LSA instead of Type-5 LSA is allowed to be injected into the Not-So-Stub-Area (NSSA). By configuring redistribution to import external routes to the NSSA area. The ASBR in the NSSA area generates Type-7 LSA and floods it to the NSSA area. The ABR in the NSSA area will convert Type-7 LSAs into Type-5 LSAs, and then flood these Type-5 LSAs to the entire AS.

The OSPF NSSA area configured through the **area area-id nssa no-summary** command is called a totally NSSA area. The OSPF totally NSSA area prohibits inter-area routes from flooding. At this time, ABR will generate a default route and flood it into the NSSA area. Devices in the NSSA area will access the networks outside the area through this default route.

Table 3 Configuring OSPF NSSA Area

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the OSPF configuration mode	<b>router ospf process-id [ vrf vrf-name ]</b>	-
Configure NSSA area	<b>area area-id nssa [ [ default-information-originate [ metric metric-value / metric-type type-value ] / no-redistribution / no-summary / suppress-fa / translator-role { always   candidate   never } ]   [ translate-always   translate-candidate   translate-never ] ]</b>	Mandatory  By default, it is not a NSSA area.



**Note**

- Backbone areas cannot be configured as NSSA areas.
- All devices in the same NSSA area must be configured as NSSA areas. Neighbor relations cannot be formed between the devices with inconsistent area types.

### Configure OSPF Stub Area

The Stub area does not allow AS external routes to flood. This can reduce the size of the link status database. After an area is configured as Stub, the ABR on the border of Stub will generate a default route and flood it into the Stub area. Devices in the Stub area will access the networks outside the AS through this default route.

The OSPF Stub area configured through the **area area-id stub no-summary** command is called a totally Stub area. The OSPF totally Stub area prohibits inter-area routes or external routes from flooding. Devices in the area will access the networks outside the area and the OSPF AS through the default route.

Table 4 Configuring OSPF Stub Area

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the OSPF configuration mode	<b>router ospf process-id [ vrf vrf-name ]</b>	-
Configure Stub area	<b>area area-id stub [ no-summary ]</b>	Mandatory By default, it is not a Stub area.
Configure ABR in the Stub area to generate the cost value of default route	<b>area area-id default-cost cost-value</b>	Optional By default, the cost value of the default route generated by ABR in the Stub area is 1.

### Note

- Backbone areas cannot be configured as Stub areas.
- All devices in the same Stub area must be configured as Stub areas. Neighbor relations cannot be formed between the devices with inconsistent area types.

## Configure OSPF Virtual Link

In OSPF, non-backbone areas must complete database synchronization and data interaction through backbone areas. Therefore, all non-backbone areas must connect with backbone areas.

When this requirement cannot be satisfied in some circumstances, you may configure a virtual link. After a virtual link is configured, you can configure authentication method and modify Hello time interval for the virtual link. Meanings of these parameters are consistent with those of general OSPF interface parameters.

Table 5 Configuring OSPF Virtual Link

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the OSPF configuration mode	<b>router ospf</b> <i>process-id</i> [ <b>vrf</b> <i>vrf-name</i> ]	-
Configure OSPF Virtual Link	<b>area</b> <i>transit-area-id</i> <b>virtual-link</b> <i>neighbor-id</i> [ [ <b>authentication</b> [ <b>key-chain</b>   <b>message-digest</b>   <b>null</b> ] <b>key-chain</b> <i>keychain-name</i>   <b>authentication-key</b> <i>key</i>   <b>message-digest-key</b> <i>key-id</i> { <b>md5</b>   <b>sm3</b> } <i>key</i> ] / <b>dead-interval</b> <i>seconds</i> <b>hello-interval</b> <i>seconds</i> / <b>retransmit-interval</b> <i>seconds</i> / <b>transmit-delay</b> <i>seconds</i> ]	Mandatory  By default, no virtual link is created.

---

### Note

- Virtual link must be configured between two ABRs.
  - The two ABRs configured with virtual links must be within the same common area, which is called the Transit Area of the virtual link.
  - This Transit Area shall not be a Stub or NSSA area.
- 

## 55.2.3 Configure OSPF Network Type

Depending on the link protocol type, OSPF divides networks into four types:

- Broadcast Networks - When the link protocol is Ethernet or FDDI, the OSPF network

type is broadcast by default;

- P2P (Point To Point Network) - When the link protocol is PPP, LAPB or HDLC, the OSPF network type is P2P by default;
- NBMA (Non-Broadcast Multi-Access Network) - When the link protocol is ATM, frame relay or X.25, the OSPF network type is NBMA by default;
- P2MP (Point To Multi-Point Network) - No link protocol will be deemed as P2MP by OSPF by default. Generally, the NBMA network which is not fully connected is configured as an OSPF P2MP.

The network type of OSPF interface can be modified as needed. The network types of the interfaces that establish OSPF neighbors must be consistent, or the normal learning of routes will be affected.

### Configuration Condition

Before configuring OSPF network type, ensure that:

- Interface IP addresses have been configured so that neighbor nodes are reachable at the network layer;
- Enable OSPF protocol.

### Configure Network Type of OSPF Interface as Broadcast

Broadcast network supports multiple (more than two) devices that can exchange information with all the devices on the network. OSPF uses Hello packets to dynamically find neighbors.

Table 6 Configuring Network Type of OSPF Interface as Broadcast

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure Network Type of OSPF Interface as Broadcast	<b>ip ospf network broadcast</b>	Mandatory  By default, the network type of OSPF interface depends on the protocol in link layer.

### Configure Network Type of OSPF Interface as P2P

Point-to-point network is the network composed of two devices, each of which is located at an end of the point-to-point link. OSPF uses Hello packets to dynamically find neighbors.

Table 55 Configuring Network Type of OSPF Interface as P2P

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure network type of OSPF as P2P	<b>ip ospf network point-to-point</b>	Mandatory  By default, the network type of OSPF interface depends on the protocol in link layer.

#### Configure Network Type of OSPF Interface as NBMA

NBMA network supports multiple (more than two) devices. Yet it cannot broadcast, and neighbors need to be manually specified.

Table 7 Configuring Network Type of OSPF Interface as NBMA

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure network type of OSPF as NBMA	<b>ip ospf network non-broadcast</b>	Mandatory  By default, the network type of OSPF interface depends on the protocol in link layer.
Enter the global configuration mode.	<b>exit</b>	-
Enter the OSPF configuration mode	<b>router ospf</b> <i>process-id</i> [ <b>vrf</b> <i>vrf-name</i> ]	-
Configure NBMA network neighbors	<b>neighbor</b> <i>neighbor-ip-address</i> [ <b>cost</b> <i>cost-value</i> / <b>priority</b> ]	Mandatory

Step	Command	Description
	<i>priority-value / poll-interval interval-value ]</i>	In NBMA network, neighbors need to be manually specified.

### Configure Network Type of OSPF Interface as P2MP

When NBMA is not fully connected, the network type can be configured as P2MP to save network cost. When the network type is configured as P2MP unicast, neighbors need to be manually specified.

Table 8 Configuring Network Type of OSPF Interface as P2MP

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure OSPF network type as P2MP	<b>ip ospf network point-to-multipoint [ non-broadcast ]</b>	Mandatory By default, the network type of OSPF interface depends on the protocol in link layer.
Enter the global configuration mode.	<b>exit</b>	-
Enter the OSPF configuration mode	<b>router ospf</b> <i>process-id</i> [ <b>vrf</b> <i>vrf-name</i> ]	-
Configure P2MP unicast network neighbors	<b>neighbor</b> <i>neighbor-ip-address</i> [ <b>cost</b> <i>cost-value</i> / <b>priority</b> <i>priority-value</i> / <b>poll-interval</b> <i>interval-value</i> ]	If the network type of interface is configured as P2MP, it is mandatory

### 55.2.4 Configure OSPF Network Authentication

In order to avoid information leakage or malicious attacks on OSPF devices, all packet interactions between OSPF neighbors can realize authentication. The authentication type can be NULL (no authentication), simple text authentication, MD5 authentication, SM3 authentication, or key-chain authentication.

After authentication is configured, when the OSPF interface receives OSPF protocol packets, authentication is required first. These packets can be received only when they pass the authentication. Therefore, for the OSPF interfaces that establish neighbor relations, their authentication method, Key ID, and authentication password must be consistent.

Authentication method and password are configured separately.

The OSPF authentication method can be configured on area, interface or interface address. In particular, area authentication has a lower priority than interface authentication which is followed by interface address authentication. That is to say, you are required to first use interface address authentication and then interface authentication and area authentication.

### Configuration Condition

Before configuring OSPF authentication, ensure that:

- Interface IP addresses have been configured so that neighbor nodes are reachable at the network layer;
- Enable OSPF protocol.

### Configure OSPF Area Authentication

OSPF area authentication simply configures the authentication method. It will completely take effect only after configuring corresponding authentication password under the interface.

Table 9 Configuring OSPF Area Authentication

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the OSPF configuration mode	<b>router ospf</b> <i>process-id</i> [ <b>vrf</b> <i>vrf-name</i> ]	-
Configure area authentication	<b>area</b> <i>area-id</i> <b>authentication</b> [ <b>message-digest</b>   <b>key-chain</b> ]	Mandatory  By default, area authentication is not configured.  In this command, configure the keyword <b>message-digest</b> which means MD5 authentication or SM3 authentication, or <b>key-chain</b> which means key-chain authentication. Otherwise, it will be

Step	Command	Description
		simple text authentication.
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure simple text authentication password	<b>ip ospf</b> [ <i>ip-address</i> ] <b>authentication-key</b> { <b>0</b>   <b>7</b> } <i>password</i>	Mandatory  By default, the simple text authentication password is not configured.
Configure MD5/SM3 authentication password	<b>ip ospf</b> [ <i>ip-address</i> ] <b>message-digest-key</b> <i>key-id</i> { <b>md5</b>   <b>sm3</b> } { <b>0</b>   <b>7</b> } <i>password</i>	Mandatory  By default, the MD5/SM3 authentication password is not configured.
Configure key-chain authentication	<b>ip ospf</b> [ <i>ip-address</i> ] <b>key-chain</b> <i>key-chain name</i>	Mandatory  By default, <b>key-chain</b> authentication is not configured.

### Configure OSPF Interface Authentication

When an OSPF interface has multiple IP addresses, you can separately specify authentication method or authentication password for an interface address. When no interface address is specified, all the addresses under the interface use the authentication method or authentication password configured.

Table 10 Configuring OSPF Interface Authentication

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure interface authentication method	<b>ip ospf</b> [ <i>ip-address</i> ] <b>authentication</b>	Mandatory

Step	Command	Description
	[ <b>key-chain</b>   <b>message-digest</b>   <b>null</b> ]	By default, no interface authentication method is configured.  In this command, configure the keyword <b>message-digest</b> which means MD5 authentication or SM3 authentication, <b>key-chain</b> which means key-chain authentication, or <b>null</b> which means no authentication. Otherwise, it will be simple text authentication.
Configure simple text authentication password	<b>ip ospf</b> [ <i>ip-address</i> ] <b>authentication-key</b> { <b>0</b>   <b>7</b> } <i>password</i>	Mandatory  By default, the simple text authentication password is not configured.
Configure MD5/SM3 authentication password	<b>ip ospf</b> [ <i>ip-address</i> ] <b>message-digest-key</b> <i>key-id</i> { <b>md5</b>   <b>sm3</b> } { <b>0</b>   <b>7</b> } <i>password</i>	Mandatory  By default, the MD5/SM3 authentication password is not configured.
Configure key-chain authentication	<b>ip ospf</b> [ <i>ip-address</i> ] <b>key-chain</b> <i>key-chain name</i>	Mandatory  By default, <b>key-chain</b> authentication is not configured.

### 55.2.5 Configure OSPF Route Generation

In OSPF, the routes in direct network segment are covered via the command **network**, external routes can be redistributed, or host routes can be added through the command **host**.

#### Configuration Condition

Before configuring OSPF route generation, ensure that:

- Interface IP addresses have been configured so that neighbor nodes are reachable at the network layer;
- Enable OSPF protocol.

### Configure OSPF Route Redistribution

When multiple routing protocols are running on a device, routes of other protocols are imported into OSPF through redistribution to generate OSPF external type-2 routes by default, with the routing metric value being 20. When external routes are imported through redistribution, you can modify the type of external route, metric, and Tag fields, and specify corresponding routing policy for route control and management.

Table 11 Configuring OSPF Route Redistribution

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the OSPF configuration mode	<b>router ospf</b> <i>process-id</i> [ <b>vrf</b> <i>vrf-name</i> ]	-
Configure OSPF Route Redistribution	<b>redistribute</b> <i>protocol</i> [ <i>protocol-id</i> ] [ <b>metric</b> <i>metric-value</i> / <b>metric-type</b> <i>metric-type</i> / <b>tag</b> <i>tag-value</i> / <b>route-map</b> <i>route-map-name</i> / <b>match</b> <i>route-type</i> ]	Mandatory  By default, no OSPF route redistribution is configured.
Configure the metric value of OSPF external route	<b>default-metric</b> <i>metric-value</i>	Optional
Configure the restriction on the number of external routes redistributed by OSPF	<b>redistribute maximum-prefix</b> <b>maximum-prefix-value</b> <b>[threshold-value [warning-only] / warning-only]</b>	Optional  By default, there is no restriction on the number of external routes redistributed by OSPF.

### Note

- When **redistribute** *protocol* [ *protocol-id* ] **metric** and **default-metric** are both configured to set the metric value of external route, the former has a higher priority.

## Configure OSPF Default Route

After the OSPF Stub area and totally NSSA area are configured, a Type-3 default route will be automatically generated. Default route cannot be automatically generated in NSSA area. But a Type-7 default route can be imported to this area through the command **area *area-id* nssa default-information-originate**.

OSPF cannot import Type-5 default route through the **redistribute** command. When necessary, the **default-information originate [always]** command can be used to achieve this purpose.

Table 12 Configuring OSPF Default Route

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the OSPF configuration mode	<b>router ospf <i>process-id</i></b> <b>[ vrf <i>vrf-name</i> ]</b>	-
Configure OSPF to import default route	<b>default-information originate [ always / metric <i>metric-value</i> / metric-type <i>metric-type</i> / route-map <i>route-map-name</i> ]</b>	Mandatory  By default, no external default route will be imported into OSPF AS.  For the default route imported, the default metric value is 1, and the type is external type-2.  <b>always</b> means that the default route is required to be generated in OSPF AS. Otherwise, it will be generated only when there is a default route in the local routing table.

## Configure OSPF Host Route

Table 13 Configuring OSPF Host Route

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Enter the OSPF configuration mode	<b>router ospf</b> <i>process-id</i> [ <b>vrf</b> <i>vrf-name</i> ]	-
Configure OSPF Host Route	<b>host</b> <i>ip-address area area-id</i> [ <b>cost</b> <i>cost</i> ]	Mandatory  By default, host route is not generated.

## 55.2.6 Configure OSPF Route Control

### Configuration Condition

Before configuring OSPF route control, ensure that:

- Interface IP addresses have been configured so that neighbor nodes are reachable at the network layer;
- Enable OSPF protocol.

### Configure OSPF Inter-area Summarization

When the ABR in OSPF advertises inter-area routes to other areas, each route is advertised separately as Type-3 LSAs. You may use the inter-area route summarization function to summarize some contiguous network segments in the area into one route to advertise the summarized route only. This can reduce the size of the OSPF database.

Table 14 Configuring OSPF Inter-area Route Summarization

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the OSPF configuration mode	<b>router ospf</b> <i>process-id</i> [ <b>vrf</b> <i>vrf-name</i> ]	-
Configure OSPF Inter-area Summarization	<b>area</b> <i>area-id range</i> <i>ip-address/mask-length</i> [ <b>advertise</b> [ <b>cost</b> <i>cost</i> ]   <b>cost</b> <i>cost</i>   <b>not-advertise</b> ]	Mandatory  By default, ABR doesn't conduct inter-area route summarization.

---

 **Note**

- The OSPF inter-area route summarization function takes effect on ABR only.
  - By default, the minimum cost value of detail routes is selected as the cost value of summarized route.
- 

### Configure OSPF External Route Summarization

When OSPF redistributes external routes, each route is advertised separately in external link status advertisement. You may use the external route summarization function to summarize some contiguous network segments outside the AS into one route to advertise the summarized route only. This can reduce the size of the OSPF database.

After configuring the command **summary-address** on ASBR, you can summarize the Type-5 LSA and Type-7 LSA within the scope of summarized address.

Table 15 Configuring OSPF External Route Summarization

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the OSPF configuration mode	<b>router ospf</b> <i>process-id</i> [ <b>vrf</b> <i>vrf-name</i> ]	-
Configure OSPF External Route Summarization	<b>summary-address</b> <i>ip-address mask</i> [ <b>not-advertise</b>   <b>tag</b> <i>tag-value</i> ]	Mandatory By default, ABR doesn't conduct external route summarization.

---

 **Note**

- The OSPF external route summarization function takes effect on ASBR only.
- 

### Configure OSPF Inter-area Route Filtration

When ABR is receiving inter-area route, ACL or prefix list is used for filtration in the incoming function; when it is advertising inter-area route, ACL or prefix list is used for filtration in the outgoing function.

Table16 Configuring OSPF Inter-area Route Filtration

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the OSPF configuration mode	<b>router ospf</b> <i>process-id</i> [ <b>vrf</b> <i>vrf-name</i> ]	-
Configure OSPF Inter-area Route Filtration	<b>area</b> <i>area-id</i> <b>filter-list</b> { <b>access</b> { <i>access-list-name</i>   <i>access-list-number</i> }   <b>prefix</b> <i>prefix-list-name</i> } { <b>in</b>   <b>out</b> }	Mandatory  By default, ABR doesn't conduct inter-area route filtration.

### Note

- When matching ACL filtration, only standard ACL is supported.
- The OSPF inter-area route filtration function takes effect on ABR only.

### Configure OSPF External Route Filtration

Configure external route filtration, i.e. apply ACL or prefix list to allow or prohibit the flooding of routes into OSPF AS from outside.

Table 17 Configuring OSPF External Route Filtration

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the OSPF configuration mode	<b>router ospf</b> <i>process-id</i> [ <b>vrf</b> <i>vrf-name</i> ]	-
Configure distribution list to filter external routes	<b>distribute-list</b> { <i>access-list-name</i>   <i>access-list-number</i>   <b>prefix</b> <i>prefix-list-name</i> } <b>out</b> [ <i>routing-protocol</i> [ <i>process-id</i> ] ]	Mandatory  By default, ASBR doesn't conduct external route filtration.

---

 **Note**

- When matching ACL filtration, only standard ACL is supported.
  - The OSPF external route filtration function takes effect on ASBR only.
- 

### Configure OSPF Route Installation Filtration

After OSPF calculates routes through LSA, the calculated OSPF protocol routing information can be filtered to prevent certain routes from being added to the routing table.

There are three ways of filtration:

- Based on prefix filtration, use ACL and prefix list to filter the destination address of route;
- Based on the next hop filtration, use prefix list to filter the next hop of route. The prefix list can also be used to filter both destination address and next hop of route at the same time;
- Based on routing policy, filter routes.

Table 18 Configuring OSPF Route Installation Filtration

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the OSPF configuration mode	<b>router ospf</b> <i>process-id</i> [ <b>vrf</b> <i>vrf-name</i> ]	-
Configure OSPF to prohibit installation of routes	<b>distribute-list</b> { <i>access-list-name</i>   <i>access-list-number</i>   <b>gateway</b> <i>prefix-list-name1</i>   <b>prefix</b> <i>prefix-list-name2</i>   <b>gateway</b> <i>prefix-list-name3</i> }   <b>route-map</b> <i>route-map-name</i> } <b>in</b> [ <i>interface-name</i> ]	Mandatory By default, the routes installed are not filtered.

---

 **Note**

- Make **prefix**, **gateway** and **route-map** filtration and ACL filtration mutually exclusive. For example, if **prefix** filtration has been configured, ACL filtration cannot be configured.
-

- Make **route-map** and **prefix** filtration and **gateway** filtration mutually exclusive.
- Make **prefix** filtration and **gateway** filtration cover each other.

### Configure Cost Value of OSPF Interface

By default, the OSPF interface cost is calculated with the following methods: reference bandwidth/interface bandwidth.

Table 19 Configuring OSPF Interface Cost Value

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure Cost Value of OSPF Interface	<b>ip ospf</b> [ <i>ip-address</i> ] <b>cost</b> <i>cost-value</i>	Optional By default, the calculation is conducted according to the reference bandwidth/interface bandwidth.

### Configure OSPF Reference Bandwidth

The reference bandwidth of interface is mainly used to calculate interface cost value which is 100Mbit/s by default. The OSPF interface cost is calculated with the following methods: reference bandwidth/interface bandwidth. When the calculation result is greater than 1, take the integer part; when it is less than 1, take 1. Therefore, in a network with a bandwidth higher than 100Mbit/s, the optimal route cannot be correctly selected. To solve this problem, the **auto-cost reference-bandwidth** command can be used to configure appropriate reference bandwidth.

Table 20 Configuring OSPF Reference Bandwidth

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Enter the OSPF configuration mode	<b>router ospf</b> <i>process-id</i> [ <b>vrf</b> <i>vrf-name</i> ]	-
Configure reference bandwidth of OSPF interface	<b>auto-cost reference-bandwidth</b> <i>reference-bandwidth</i>	Optional By default, the reference bandwidth is 100Mbit/s.

### Configure OSPF Administrative Distance

Administrative distance indicates the reliability of routing protocol. When the routes that reach the same destination network are learned from different routing protocols, they are selected according to the administrative distance. Those with a small administrative distance are selected first.

Table 21 Configuring OSPF Administrative Distance

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the OSPF configuration mode	<b>router ospf</b> <i>process-id</i> [ <b>vrf</b> <i>vrf-name</i> ]	-
Configure OSPF Administrative Distance	<b>distance</b> { <i>distance</i> [ <i>ip-address wildcard-mask</i> ] [ <i>access-list-name</i>   <i>access-list-number</i> ]   <b>ospf</b> { <b>external</b> <i>distance</i>   <b>inter-area</b> <i>distance</i>   <b>intra-area</b> <i>distance</i> } }	Optional By default, the administrative distance of intra-area and inter-area routes of OSPF is 110, and that of external routes is 150.

### Configure the Maximum Number of Load Balancing Entries of OSPF

If there are multiple equal-cost paths leading to the same destination address, the paths form load balancing, which can improve the link utility rate and reduce the load of links.

Table 22 Configuring Maximum Number of OSPF Load Balancing Entries

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the OSPF configuration mode	<b>router ospf</b> <i>process-id</i> [ <b>vrf</b> <i>vrf-name</i> ]	-
Configure the Maximum Number of Load Balancing Entries of OSPF	<b>maximum-path</b> <i>max-number</i>	Optional By default, the maximum number of OSPF load balancing entries is 4.

### Configure OSPF to be Compatible with RFC1583

When there are multiple paths that reach ASBR or external route forwarding address, RFC1583 and RFC2328 define different routing rules. To be compatible with RFC1583, first select the intra-area or inter-area paths within the backbone area; to be incompatible with RFC1583, first select the intra-area paths within the non-backbone area.

Table 23 Configuring OSPF Compatible with RFC1583

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the OSPF configuration mode	<b>router ospf</b> <i>process-id</i> [ <b>vrf</b> <i>vrf-name</i> ]	-
Configure OSPF to be Compatible with RFC1583	<b>compatible rfc1583</b>	Mandatory By default, it is incompatible with RFC1583.

### Note

- In OSFP AS, all devices must have the same routing rules. Namely, they shall all be either compatible with or incompatible with RFC1583 to avoid routing loops.

## 55.2.7 Configure OSPF Network Optimization

### Configuration Condition

Before configuring OSPF network optimization, ensure that:

- Interface IP addresses have been configured so that neighbor nodes are reachable at the network layer;
- Enable OSPF protocol.

### Configure Keepalive Time of OSPF Neighbors

OSPF Hello packets are used to establish and keep alive neighbor relations. The default time interval of sending Hello packets depends on the network type. In broadcast and P2P networks, it is 10 seconds, and in P2MP and NBMA networks, it is 30 seconds.

The failure time of neighbor is used to identify the validity of the neighbor. By default, it is 4 times the Hello time interval. If the OSPF device does not receive the Hello packets from the neighbor after time out of its failure time, the neighbor is considered invalid and deleted.

Table 24 Configuring OSPF Neighbor Keepalive Time

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure OSPF Hello interval	<b>ip ospf</b> [ <i>ip-address</i> ] <b>hello-interval</b> <i>interval-value</i>	Optional The default value is determined based on network class. For broadcast and P2P networks, it's 10 seconds; for P2MP and NBMA networks, it's 30 seconds.
Configure failure time of OSPF neighbors	<b>ip ospf</b> [ <i>ip-address</i> ] <b>dead-interval</b> <i>interval-value</i>	Optional The default value is 4 times the Hello interval.

---

 **Note**

- The Hello interval between adjacent OSPF devices must be the same as the failure time of neighbor. Otherwise, neighbor relation cannot be established.
  - When modifying Hello interval, if the failure time of current neighbor is 4 times the Hello interval, the failure time of neighbor will also be automatically modified so that it is 4 times the Hello interval; if the failure time of current neighbor is not 4 times the Hello interval, the failure time of neighbor will remain unchanged.
  - Modifying the failure time of neighbor will not affect the Hello interval.
- 

### Configure Passive OSPF Interface

Dynamic routing protocol uses passive interface, which can effectively reduce the consumption of network bandwidth by routing protocol. Configure passive OSPF interface to advertise the route of the direct network segment where the interface is located through the command **network**. But it will suppress the receiving and sending of OSPF protocol packets on this interface.

Table 25 Configuring Passive OSPF Interface

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the OSPF configuration mode	<b>router ospf process-id [ vrf vrf-name ]</b>	-
Configure Passive OSPF Interface	<b>passive-interface { interface-name [ ip-address ]   default }</b>	Mandatory By default, no passive OSPF interface is configured.

### Configure OSPF Demand Circuit

On P2P and P2MP links, to reduce line costs, you can configure OSPF demand circuit to suppress the periodic sending of Hello packets and periodic refresh of LSA packets. It is mainly applied in paid links, such as ISDN, SVC and X.25.

Table 26 Configuring OSPF Demand Circuit

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure OSPF Demand Circuit	<b>ip ospf</b> [ <i>ip-address</i> ] <b>demand-circuit</b>	Mandatory By default, the OSPF demand circuit is disabled.

### Configure OSPF Interface Priority

Interface priority is mainly applied in the election of DR (Designed Router) and BDR (Backup Designed Router) in broadcast and NBMA networks. The value ranges from 0 to 255. The larger the value, the higher the priority. The default value is 1.

DR and BDR are elected by all the devices in the same network segment according to interface priority and Router ID through Hello packets. The rules are shown below:

- Firstly, the device with the highest interface priority is elected as the DR, and that with the second interface priority as the BDR. The device with the priority of 0 does not participate in the election;
- If the interface priorities are the same, the device with the highest router ID is elected as the DR, and that with the second router ID as the BDR;
- After the DR fails, BRD will become a DR immediately, and a new BDR will be elected.

Table 27 Configuring OSPF Interface Priority

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure OSPF Interface Priority	<b>ip ospf priority</b> <i>priority-value</i>	Optional By default, the OSPF interface priority is 1.

---

 **Note**

- Priority affects the election process only. When DR and BDR have been elected in the network, modifying interface priority will affect the next election result only. Therefore, DR is not necessarily the device with the highest interface priority, and DBR is not necessarily the device with the second high interface priority.
- 

### Configure OSPF Interface MTU

When encapsulating OSPF packets, to avoid fragmentation, the packet size must be no more than the MTU value of interface. When adjacent OSPF devices exchange DD packets with each other, they will check whether the MTUs are the same by default. If different, a neighbor relation cannot be established. After OSPF is configured to ignore interface MTU check, even if the MTUs are different, the neighbor relation can be established.

Table 28 Configuring OSPF Interface MTU

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure OSPF Interface MTU	<b>ip ospf mtu</b> <i>mtu-value</i>	Optional
Configure OSPF Interface to ignore MTU consistency check	<b>ip ospf</b> [ <i>ip-address</i> ] <b>mtu-ignore</b>	Mandatory By default, MTU check will be conducted. consistency check

### Configure Transfer Delay of OSPF Interface

LSA transfer delay means the period during which LSA floods to other devices. The device sending LSA will add the interface transfer delay time to the aging time of the LSA to be sent. By default, when the flooded LSA passes through a device, the aging time increases by 1. The transfer delay of LSA can be configured according to network conditions, from 1 to 840. It is generally used on low-speed links.

Table 29 Configuring OSPF Interface LSA Transfer Delay

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure Transfer Delay of OSPF Interface	<b>ip ospf transmit-delay</b> <i>delay-value</i>	Optional By default, the LSA transfer delay is 1 second.

### Configure OSPF LSA Retransmission

In order to ensure the reliability of data interaction, OSPF uses the acknowledgement mechanism. When an LSA is flooded on the device interface, it will be added to the neighbor's retransmission list. If confirmation is not received from the neighbor after the retransmission time expires, this LSA will be retransmitted until the confirmation is received.

Table 30 Configuring OSPF LSA Redistribution

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure OSPF LSA retransmission interval	<b>ip ospf retransmit-interval</b> <i>interval-value</i>	Optional By default, the retransmission interval is 5 seconds.
Enter the global configuration mode.	<b>exit</b>	-
Enter the OSPF configuration mode	<b>router ospf</b> <i>process-id</i> [ <b>vrf</b> <i>vrf-name</i> ]	-
Configure OSPF LSA retransmission queue scanning interval	<b>timers lsa retransmission scan-time</b>	Optional By default, the retransmission queue

Step	Command	Description
		scanning interval is 1250 milliseconds.

### Configure OSPF to Prohibit LSA Diffusion

In practical network applications, redundant links are used between OSPF neighbors sometimes. This configuration can reduce the spreading of OSPF update packets on redundant links.

Table 31 Configuring OSPF to Prohibit LSA Diffusion

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure OSPF interface to prohibit LS-UPD diffusion	<b>ip ospf database-filter all out</b>	Mandatory By default, OSPF interface doesn't prohibit LSA diffusion.

### Note

- Configuring OSPF to prohibit LSA diffusion may result in loss of some routing information.

### Configure OSPF SPF Calculation Time

When the OSPF network topology changes, recalculation of routes is required. When the network keeps changing, frequent routing calculation will occupy a large amount of system resources. The consumption of system resources by frequent network changes can be suppressed by adjusting the time parameters of SPF calculation.

Table 32 Configuring OSPF SPF Calculation Time

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the OSPF configuration mode	<b>router ospf</b> <i>process-id</i> [ <b>vrf</b> <i>vrf-name</i> ]	-
Configure OSPF SPF Calculation Time	<b>timers throttle spf</b> <i>delay-time</i> <i>hold-time</i> <i>max-time</i>	Optional  By default, the delay-time, hold-time and max-time are 5000 ms, 10000 ms, and 10000 ms, respectively.

## Note

- *Delay-time* means the initial calculation delay, *hold-time* the suppression time, and *max-time* the maximum waiting time for two SPF calculations. When there are infrequent network changes, the continuous route calculation interval is decreased to *delay-time*. In the case of frequent network changes, adjustment should be made accordingly by increasing the *hold-time* × 2<sup>n-2</sup> (n is the times of continuously triggering route calculation) to prolong the waiting time by the increment of the *hold-time* configured, *max-time* at most.

## Configure OSPF Database Overflow

OSPF database overflow is used to restrict the number of Type-5 LSA in the database.

Table 33 Configuring OSPF Database Overflow

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the OSPF configuration mode	<b>router ospf</b> <i>process-id</i> [ <b>vrf</b> <i>vrf-name</i> ]	-
Configure OSPF Database Overflow	<b>overflow database external</b> <i>max-number</i> <i>seconds</i>	Mandatory  By default, the OSPF database overflow function is disabled.

---

## Caution

- Enabling the database overflow function may cause inconsistency between the databases in the OSPF area and loss of some routes.
- 

### 55.2.8 Configure OSPF to Coordinate with BFD

#### Configuration Condition

Before configuring the coordination of OSPF with BFD, ensure that:

- Interface IP addresses have been configured so that neighbor nodes are reachable at the network layer;
- Enable OSPF protocol.

#### Configure OSPF to Coordinate with BFD

BFD (Bidirectional Forwarding Detection) provides a method to quickly detect the status of lines between two devices. When BFD detection is enabled between two adjacent OSPF devices, if there is a line failure between the devices, BFD can quickly detect the failure and notify the OSPF protocol to trigger OSPF for route calculation and switch to the backup route. In this way, it can reach the purpose of fast route switch.

Table 34 Configuring OSPF to Coordinate with BFD

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure the specified OSPF interface to enable or disable BFD	<b>ip ospf bfd</b> [ <i>ip-address</i> / <b>disable</b> ]	Mandatory By default, the BFD function is not enabled.
Enter the global configuration mode.	<b>exit</b>	-
Enter the OSPF configuration mode	<b>router ospf</b> <i>process-id</i> [ <b>vrf</b> <i>vrf-name</i> ]	-

Step	Command	Description
Configure all interfaces of OSPF process to enable BFD	<b>bfd all-interfaces</b>	Optional

## Note

- When BFD is configured in OSPF configuration mode and interface configuration mode at the same time, the latter has a higher priority.

### 55.2.9 Configure OSPF FRR

#### Configuration Condition

Before configuring OSPF FRR, ensure that:

- Interface IP addresses have been configured so that neighbor nodes are reachable at the network layer.
- Enable OSPF protocol.

#### Configure OSPF FRR

In the OSPF network, as a result of link or device failure, the packets passing the point of failure will be discarded or loops will be produced. The traffic interruption caused thereby will continue until the protocol reconverges after several seconds. In order to reduce the time of traffic interruption, OSPF FRR can be configured. By applying the routing map, set a backup next hop for the successfully matched route. Once the main link fails, the traffic passing through the failed link will immediately switch to the backup link, achieving the purpose of fast switching.

Table 35 Configuring OSPF FRR

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the OSPF configuration mode	<b>router ospf</b> <i>process-id</i> [ <b>vrf</b> <i>vrf-name</i> ]	-
Configure OSPF process to enable the FRR function	<b>fast-reroute route-map</b> <i>route-map-name</i>	Mandatory By default, the OSPF FRR function is disabled.

Step	Command	Description
Configure OSPF process to enable the dynamic FRR function	<b>fast-reroute loop-free-alternate</b> [route-map <i>route-map-name</i> ]	Mandatory By default, the OSPF dynamic FRR function is disabled.
Configure OSPF process to enable the pic function	<b>pic</b>	Mandatory After the pic function is enabled, the auto FRR function is enabled.  By default, the OSPF pic function is disabled.

---

### Note

- The OSPF FRR function has two types, i.e. static FRR and dynamic FRR.
  - Static FRR needs to associate route-map where the next hop interface and address of back-up route are set.
  - Currently, dynamic FRR supports point-to-point network only, i.e. all the output interfaces of the device have a network type of point-to-point. After dynamic FRR is configured, the device automatically calculates and sets back-up next hop interface and address. Dynamic FRR can also associate route-map to set back-up next hop interface and address for the route which matches the route-map only.
  - The methods of enabling route redistribution are mutually exclusive.
- 

## 55.2.10 Configure OSPF GR

GR (Graceful Restart) is used to keep the routing information in the forwarding layer of this device and neighbor device unchanged during the switch between host and standby devices to ensure the forwarding process is not affected; after the device is switched for re-running, the two devices synchronize routing information and update forwarding layer in the protocol layer so that the data can keep forwarding during the process of device switch.

There are two types of roles in the GR process:

- GR Restarter end: The device for graceful restart of protocol.
- GR Helper end: The device which helps with the graceful restart of protocol.

The distributed device can act as GR Restarter and GR Helper, while the centralized device only serves as GR Helper to help the Restarter complete GR.

### Configuration Condition

Before configuring OSPF GR, ensure that:

- Configure interface IP addresses so that neighbor nodes are reachable.
- Enable OSPF protocol.

### Configure OSPF GR Restarter

Table 36 Configuring OSPF GR Restarter

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the OSPF configuration mode	<b>router ospf</b> <i>process-id</i> [ <b>vrf</b> <i>vrf-name</i> ]	-
Configure OSPF GR	<b>nsf ietf</b>	Mandatory  By default, the GR function is disabled.  After this function takes effect, the protocol needs to support the Opaque-LSA function, and it supports the Opaque-LSA function by default.
Configure OSPF GR period	<b>nsf interval</b> <i>grace-period</i>	Optional  By default, the GR period is 95 seconds.
Configure OSPF GR proxy	<b>graceful-restart proxy</b>	Optional  By default, the OSPF GR proxy is enabled.  GR Proxy means that GR packets are prepared before switching, and you don't have to wait for OSPF to start after switching before sending

Step	Command	Description
		GR packets to keep OSPF neighbors alive.

## Note

- The OSPF GR function can only be used in the stacking environment or a dual-master environment.

### Configure OSPF GR Helper

GR Helper can help the Restarter end complete GR. By default, the device enables this function. Users can disable this function via the command **nsf ietf helper disable**. The command **nsf ietf helper strict-lsa-checking** is used to enable the Helper end to strictly check LSA in the GR process. If any change of LSA is found, the GR Helper mode will be exited.

Table 37 Configuring OSPF GR Helper

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the OSPF configuration mode	<b>router ospf</b> <i>process-id</i> [ <b>vrf</b> <i>vrf-name</i> ]	-
Configure OSPF GR Helper	<b>nsf ietf helper</b> [ <b>disable</b>   <b>strict-lsa-checking</b> ]	Optional By default, the Helper function is enabled, but it doesn't check LSA.

### 55.2.11 OSPF monitoring and maintaining

Table 38 OSPF Monitoring and Maintaining

Command	Description
<b>clear ip ospf</b> [ <i>process-id</i> ] <b>process</b>	Reset OSPF process

Command	Description
<b>clear ip ospf process-id neighbor neighbor-ip-address [ neighbor-router-id ]</b>	Reset OSPF neighbors
<b>clear ip ospf statistics [ interface-name ]</b>	Clear interface statistics of OSPF
<b>clear ip ospf [ process-id ] redistribution</b>	Re-advertise external route
<b>clear ip ospf [ process-id ] route</b>	Recalculate OSPF route
<b>show ip ospf [ process-id ]</b>	Show basic information of OSPF
<b>show ip ospf [ process-id ] border-routers</b>	Show information of the route reaching edge device in OSPF
<b>show ip ospf [ process-id ] buffers</b>	Show size of OSPF packet sending and receiving cache
<b>show ip ospf [ process-id ] database [ adv-router router-id   database-summary   max-age   [ asbr-summary   external   network   nssa-external   opaque-area   opaque-as   opaque-link   router   self-originate   summary ] [ [ link-state-id ] [ adv-router advertising-router-id ]   self-originate   summary ] ]</b>	Show the information of OSPF database
<b>show ip ospf interface [ interface-name [ detail ] ]</b>	Show OSPF interface information
<b>show ip ospf [ process-id ] neighbor [ neighbor-id   all   detail [ all ]   interface ip-address [ detail ]   statistic ]</b>	Show the information of OSPF neighbors
<b>show ip ospf [ process-id ] route [ ip-address mask   ip-address/mask-length   external   inter-area   intra-area   statistic ]</b>	Show the routing information of OSPF protocol
<b>show ip ospf [ process-id ] virtual-links</b>	Show the information of OSPF virtual link
<b>show ip ospf [ process-id ] sham-links</b>	Show the OSPF pseudo-class link interface information configured, including interface status, cost value, and neighbor status

## 55.3 Typical configuration example of OSPF

### 55.3.1 Configure OSPF Basic Functions

#### Network Requirements

- All devices are configured with OSPF protocol, and there are three areas, i.e. area 0, 1 and 2. Upon completion of the configuration, all the devices can learn routes from each other.
- On the back-to-back Ethernet interface, in order to speed up the the process of establishing OSPF neighbors, the network type of OSPF interface can be changed to point-to-point. Modify the network type of the interface in area 2 as point-to-point. Upon completion of the configuration, all the devices can learn routes from each other.

#### Network Topology

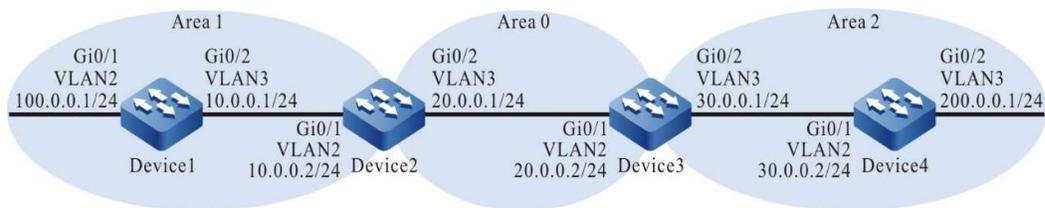


Figure 55-1 Network Topology for Configuring Basic Functions of OSPF

#### Configuration Steps

- Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)
- Step 2: Configures IP addresses for the ports. (Omitted)
- Step 3: Configure OSPF process and make different areas cover corresponding interfaces.

#On Device1, configure OSPF process and make area 1 cover the interface.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#router-id 1.1.1.1
Device1(config-ospf)#network 10.0.0.0 0.0.0.255 area 1
Device1(config-ospf)#network 100.0.0.0 0.0.0.255 area 1
Device1(config-ospf)#exit
```

#On Device2, configure OSPF process and make area 0 and 1 cover corresponding interfaces.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#router-id 2.2.2.2
Device2(config-ospf)#network 20.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#network 10.0.0.0 0.0.0.255 area 1
Device2(config-ospf)#exit
```

#On Device3, configure OSPF process and make area 0 and 2 cover corresponding interfaces.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#router-id 3.3.3.3
Device3(config-ospf)#network 20.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 30.0.0.0 0.0.0.255 area 2
Device3(config-ospf)#exit
```

#On Device4, configure OSPF process and make area 2 cover the interface.

```
Device4#configure terminal
Device4(config)#router ospf 100
Device4(config-ospf)#router-id 4.4.4.4
Device4(config-ospf)#network 30.0.0.0 0.0.0.255 area 2
Device4(config-ospf)#network 200.0.0.0 0.0.0.255 area 2
Device4(config-ospf)#exit
```

---

## Note

- Router ID can be manually configured or automatically generated. If the Router ID is not manually configured, the device will automatically select it. The largest IP address in Loopback interfaces is first selected as Router ID; if no Loopback interface address is configured on the device, the largest IP address in general interfaces is selected as Router ID. Only when the interface is up can the interface address be selected as Router ID.
  - When using the command **network**, the reverse mask doesn't have to accurately match the length of the interface IP address mask. The network segment **network** simply needs to cover the interface IP address. For example, **network 0.0.0.0 255.255.255.255** means all the interfaces are covered.
- 

#View OSPF neighbors' information and routing table on Device1.

```
Device1#show ip ospf neighbor
OSPF process 100:
Neighbor ID  Pri  State      Dead Time  Address    Interface
2.2.2.2      1  Full/DR   00:00:36  10.0.0.2   vlan3

Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 10.0.0.0/24 is directly connected, 02:26:21, vlan3
O 20.0.0.0/24 [110/2] via 10.0.0.2, 02:25:36, vlan3
O 30.0.0.0/24 [110/3] via 10.0.0.2, 02:25:36, vlan3
C 100.0.0.0/24 is directly connected, 02:26:23, vlan2
C 127.0.0.0/8 is directly connected, 18:09:44, lo0
O 200.0.0.0/24 [110/4] via 10.0.0.2, 02:25:36, vlan3
```

#View the OSPF neighbors and routing table on Device2.

```
Device2#show ip ospf neighbor
OSPF process 100:
Neighbor ID  Pri  State      Dead Time  Address    Interface
1.1.1.1      1  Full/Backup 00:00:37  10.0.0.1   vlan2
3.3.3.3      1  Full/DR   00:00:38  20.0.0.2   vlan3

Device2#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
```

U - Per-user Static route  
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 10.0.0.0/24 is directly connected, 02:31:15, vlan2  
C 20.0.0.0/24 is directly connected, 02:31:50, vlan3  
O 30.0.0.0/24 [110/2] via 20.0.0.2, 02:31:40, vlan3  
O 100.0.0.0/24 [110/2] via 10.0.0.1, 02:30:29, vlan2  
C 127.0.0.0/8 is directly connected, 240:21:34, lo0  
O 200.0.0.0/24 [110/3] via 20.0.0.2, 02:31:40, vlan3

## #View the OSPF LSDB (Link State Database) on Device2.

```
Device2#show ip ospf database
```

OSPF Router with ID (2.2.2.2) (Process ID 100)

Router Link States (Area 0)

Link ID	ADV Router	Age	Seq#	CkSum	Link count
2.2.2.2	2.2.2.2	1777	0x8000000c	0xcb20	1
3.3.3.3	3.3.3.3	309	0x8000000a	0x9153	1

Net Link States (Area 0)

Link ID	ADV Router	Age	Seq#	CkSum
20.0.0.2	3.3.3.3	369	0x80000006	0xec12

Summary Link States (Area 0)

Link ID	ADV Router	Age	Seq#	CkSum	Route
10.0.0.0	2.2.2.2	1757	0x80000005	0xcc59	10.0.0.0/24
100.0.0.0	2.2.2.2	1356	0x80000005	0x408a	100.0.0.0/24
30.0.0.0	3.3.3.3	9	0x80000006	0xa765	30.0.0.0/24
200.0.0.0	3.3.3.3	149	0x80000006	0x075a	200.0.0.0/24

Router Link States (Area 1)

Link ID	ADV Router	Age	Seq#	CkSum	Link count
1.1.1.1	1.1.1.1	1775	0x80000009	0xbbda	2
2.2.2.2	2.2.2.2	1737	0x80000008	0x2dd5	1

Net Link States (Area 1)

Link ID	ADV Router	Age	Seq#	CkSum
10.0.0.2	2.2.2.2	34	0x80000006	0x39db

Summary Link States (Area 1)

Link ID	ADV Router	Age	Seq#	CkSum	Route
20.0.0.0	2.2.2.2	144	0x80000006	0x48d2	20.0.0.0/24
30.0.0.0	2.2.2.2	1186	0x80000005	0xd13f	30.0.0.0/24
200.0.0.0	2.2.2.2	14	0x80000006	0x2f35	200.0.0.0/24

For Device2, both 30.0.0.0/24 and 200.0.0.0/24 are inter-area routes. LSA information of relevant routes can be seen from Summary Link States (Area 0). For intra-area route, **show ip ospf database router** is required to see the LSA information of relevant routes.

Step 4: Configure the network type of OSPF interface as point-to-point.

#On Device3, change the OSPF network type of VLAN3 to point-to-point.

```
Device3(config)#interface vlan3  
Device3(config-if-vlan3)#ip ospf network point-to-point  
Device3(config-if-vlan3)#exit
```

#On Device4, change the OSPF network type of VLAN2 to point-to-point.

```
Device4(config)#interface vlan2
Device4(config-if-vlan2)#ip ospf network point-to-point
Device4(config-if-vlan2)#exit
```

Step 5: Check the result.

#View the OSPF neighbors and routing table on Device3.

```
Device3#show ip ospf neighbor
OSPF process 100:
Neighbor ID Pri State Dead Time Address Interface
2.2.2.2 1 Full/Backup 00:00:36 20.0.0.1 vlan2
4.4.4.4 1 Full/- 00:00:39 30.0.0.2 vlan3

Device3#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
U - Per-user Static route
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

O 10.0.0.0/24 [110/2] via 20.0.0.1, 00:02:53, vlan2
C 20.0.0.0/24 is directly connected, 03:20:36, vlan2
C 30.0.0.0/24 is directly connected, 03:20:26, vlan3
O 100.0.0.0/24 [110/3] via 20.0.0.1, 00:01:51, vlan2
C 127.0.0.0/8 is directly connected, 262:01:24, lo0
O 200.0.0.0/24 [110/2] via 30.0.0.2, 00:00:11, vlan3
```

---

## Note

- When OSPF neighbor relations are established in point-to-point networks, there is no DR or BDR election.
- 

#View the OSPF neighbors and routing table on Device4.

```
Device4#show ip ospf neighbor
OSPF process 100:
Neighbor ID Pri State Dead Time Address Interface
3.3.3.3 1 Full/- 00:00:39 30.0.0.1 vlan2

Device4#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
U - Per-user Static route
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

O 10.0.0.0/24 [110/3] via 30.0.0.1, 00:01:04, vlan2
O 20.0.0.0/24 [110/2] via 30.0.0.1, 00:01:04, vlan2
C 30.0.0.0/24 is directly connected, 03:20:25, vlan2
O 100.0.0.0/24 [110/4] via 30.0.0.1, 00:01:04, vlan2
C 127.0.0.0/8 is directly connected, 22:52:36, lo0
C 200.0.0.0/24 is directly connected, 03:20:13, vlan3
```

According to the result, after the network type of OSPF interface is changed to point-to-point, neighbors can be normally established, and routes can be learned normally.

---

## Note

- When the network type of OSPF interface is configured, the network type of OSPF interfaces at both sides of the neighbor must be consistent. Otherwise, it will affect the normal learning and flooding of route. By default, the network type of OSPF interface depends on the network type of physical interface.
- 

### 55.3.2 Configure OSPF authentication

#### Network Requirements

- OSPF is running on all devices that are configured with area authentication. Area 0 is configured with simple text authentication, and area 1 with MD5 authentication.
- Configure OSPF interface authentication: simple text authentication for area 0 and MD5 authentication for area 1.
- Upon completion of the configuration, the device can normally establish neighbors and learn routes from each other.

#### Network Topology



Figure 55-2 Network Topology for Configuring OSPF Authentication

#### Configuration Steps

- Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)
- Step 2: Configures IP addresses for the ports. (Omitted)
- Step 3: Configure OSPF process, make different areas cover corresponding interfaces, and enable area authentication. In particular, area 0 uses simple text authentication, and area 1 MD5 authentication.

#On Device1, configure OSPF process and area authentication function.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#router-id 1.1.1.1
Device1(config-ospf)#area 0 authentication
```

```
Device1(config-ospf)#network 10.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#exit
```

#On Device2, configure OSPF process and area authentication function.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#router-id 2.2.2.2
Device2(config-ospf)#area 0 authentication
Device2(config-ospf)#area 1 authentication message-digest
Device2(config-ospf)#network 10.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#network 20.0.0.0 0.0.0.255 area 1
Device2(config-ospf)#exit
```

#On Device3, configure OSPF process and area authentication function.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#router-id 3.3.3.3
Device3(config-ospf)#area 1 authentication message-digest
Device3(config-ospf)#network 20.0.0.0 0.0.0.255 area 1
Device3(config-ospf)#exit
```

#View the information of OSPF process on Device1.

```
Device1#show ip ospf 100
Routing Process "ospf 100" with ID 1.1.1.1
Process bound to VRF default
Process uptime is 30 minutes
IETF NSF restarter support disabled
IETF NSF helper support enabled
Conforms to RFC2328, and RFC1583Compatibility flag is disabled
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Graceful Restart
Initial SPF schedule delay 5000 msec
Minimum hold time between two consecutive SPFs 10000 msec
Maximum wait time between two consecutive SPFs 10000 msec
Refresh timer 10 secs
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of non-default external LSA is 0
External LSA database is unlimited.
Not Support Demand Circuit lsa number is 0, autonomy system support flood DoNotAge Lsa
Number of areas attached to this router: 1
  Area 0 (BACKBONE)   Number of interfaces in this area is 1(1)
    Number of fully adjacent neighbors in this area is 1
    Number of fully adjacent sham-link neighbors in this area is 0
    Area has simple password authentication
    SPF algorithm last executed 00:27:43.916 ago
    SPF algorithm executed 3 times
    Number of LSA 4. Checksum Sum 0x0160f7
    Not Support Demand Circuit lsa number is 0,
    Indication lsa (by other routers) number is: 0,
    Area support flood DoNotAge Lsa
```

According to the result, area authentication is a simple text method.

#View OSPF neighbors' information and routing table on Device1.

```
Device1#show ip ospf neighbor
OSPF process 100:
Neighbor ID   Pri  State           Dead Time  Address      Interface
2.2.2.2       1    Full/DR         00:00:38  10.0.0.2    vlan2

Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
U - Per-user Static route
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```

C 10.0.0.0/24 is directly connected, 00:14:01, vlan2
O 20.0.0.0/24 [110/2] via 10.0.0.2, 00:10:38, vlan2
C 127.0.0.0/8 is directly connected, 20:55:08, lo0

```

On Device1, neighbors are normally established, and route learning is normal.

#View OSPF process information on Device3.

```

Device3#show ip ospf 100
Routing Process "ospf 100" with ID 3.3.3.3
Process bound to VRF default
Process uptime is 28 minutes
IETF NSF restarter support disabled
IETF NSF helper support enabled
Conforms to RFC2328, and RFC1583Compatibility flag is disabled
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Graceful Restart
Initial SPF schedule delay 5000 msec
Minimum hold time between two consecutive SPF's 10000 msec
Maximum wait time between two consecutive SPF's 10000 msec
Refresh timer 10 secs
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of non-default external LSA is 0
External LSA database is unlimited.
Not Support Demand Circuit lsa number is 0, autonomy system support flood DoNotAge Lsa
Number of areas attached to this router: 1
  Area 1   Number of interfaces in this area is 1(1)
    Number of fully adjacent neighbors in this area is 1
    Number of fully adjacent sham-link neighbors in this area is 0
    Number of fully adjacent virtual neighbors through this area is 0
    Area has message digest authentication
    SPF algorithm last executed 00:24:01.783 ago
    SPF algorithm executed 5 times
    Number of LSA 4. Checksum Sum 0x0337cf
    Not Support Demand Circuit lsa number is 0,
    Indication lsa (by other routers) number is: 0,
    Area support flood DoNotAge Lsa

```

According to the result, area authentication is a MD5 authentication method.

#View OSPF neighbors' information and routing table on Device3.

```

Device3#show ip ospf neighbor
OSPF process 100:
Neighbor ID  Pri  State      Dead Time  Address    Interface
2.2.2.2      1  Full/Backup  00:00:33  20.0.0.1  vlan2

Device3#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

O 10.0.0.0/24 [110/2] via 20.0.0.1, 00:09:31, vlan2
C 20.0.0.0/24 is directly connected, 00:20:36, vlan2
C 127.0.0.0/8 is directly connected, 24:00:06, lo0

```

On Device3, neighbors are normally established, and route learning is normal.

Step 4: Configure OSPF interface authentication.

#On Device1, the interface VLAN2 uses simple text authentication, with the password being admin.

```

Device1(config)#interface vlan2
Device1(config-if-vlan2)#ip ospf authentication

```

```
Device1(config-if-vlan2)#ip ospf authentication-key 0 admin
Device1(config-if-vlan2)#exit
```

#On Device2, the interface VLAN2 uses simple text authentication, with the password being admin; the interface VLAN3 uses MD5 authentication, with the Key ID being 1 and the password being admin.

```
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ip ospf authentication
Device2(config-if-vlan2)#ip ospf authentication-key 0 admin
Device2(config-if-vlan2)#exit
Device2(config)#interface vlan3
Device2(config-if-vlan3)#ip ospf authentication message-digest
Device2(config-if-vlan3)#ip ospf message-digest-key 1 md5 0 admin
Device2(config-if-vlan3)#exit
```

#On Device3, the interface VLAN2 uses MD5 authentication, with the Key ID being 1 and the password being admin.

```
Device3(config)#interface vlan2
Device3(config-if-vlan2)#ip ospf authentication message-digest
Device3(config-if-vlan2)#ip ospf message-digest-key 1 md5 0 admin
Device3(config-if-vlan2)#exit
```

Step 5: Check the result.

#View the information of OSPF neighbors on Device2.

```
Device2#show ip ospf neighbor
OSPF process 100:
Neighbor ID  Pri  State      Dead Time  Address      Interface
1.1.1.1      1  Full/Backup  00:00:33  10.0.0.1    vlan2
3.3.3.3      1  Full/DR     00:00:39  20.0.0.2    vlan3
```

#View the information of OSPF interface on Device2.

```
Device2#show ip ospf interface vlan2
vlan2 is up, line protocol is up
Internet Address 10.0.0.2, 10.0.0.255( a[10.0.0.2] d[10.0.0.255]) Area 0, MTU 1500
Process ID 100, Router ID 2.2.2.2, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DR, Priority 1, TE Metric 0
Designated Router (ID) 2.2.2.2, Interface Address 10.0.0.2
Backup Designated Router (ID) 1.1.1.1, Interface Address 10.0.0.1
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:04
Neighbor Count is 1, Adjacent neighbor count is 1
Crypt Sequence Number is 0
Graceful restart proxy id is 0x0
Hello received 406 sent 454, DD received 8 sent 6
LS-Req received 2 sent 2, LS-Upd received 11(LSA: 15) sent 10(LSA: 14)
LS-Ack received 10 sent 0, Discarded 0
```

```
Device2#show ip ospf interface vlan3
vlan3 is up, line protocol is up
Internet Address 20.0.0.1, 20.0.0.255( a[20.0.0.1] d[20.0.0.255]) Area 1, MTU 1500
Process ID 100, Router ID 2.2.2.2, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State Backup, Priority 1, TE Metric 0
Designated Router (ID) 3.3.3.3, Interface Address 20.0.0.2
Backup Designated Router (ID) 2.2.2.2, Interface Address 20.0.0.1
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:00
Neighbor Count is 1, Adjacent neighbor count is 1
Crypt Sequence Number is 485
Graceful restart proxy id is 0x0
Hello received 412 sent 454, DD received 9 sent 12
LS-Req received 3 sent 3, LS-Upd received 9(LSA: 10) sent 13(LSA: 16)
```

Crypt Sequence Number will be generated after configuring MD5 authentication; simple text authentication doesn't generate this sequence number.

---

## Note

- When configuring OSPF authentication, you can configure area authentication or interface authentication only, or configure both area and interface authentication.
  - When area authentication and interface authentication are configured at the same time, the latter takes effect first.
- 

### 55.3.3 Configure OSPF Route Redistribution

#### Network Requirements

- OSPF protocol is run between Device1 and Device2, and RIPv2 protocol is run between Device2 and Device3.
- Device2 redistributes RIP route to OSPF, and uses routing policy control to redistribute the route 100.0.0.0/24 only.

#### Network Topology

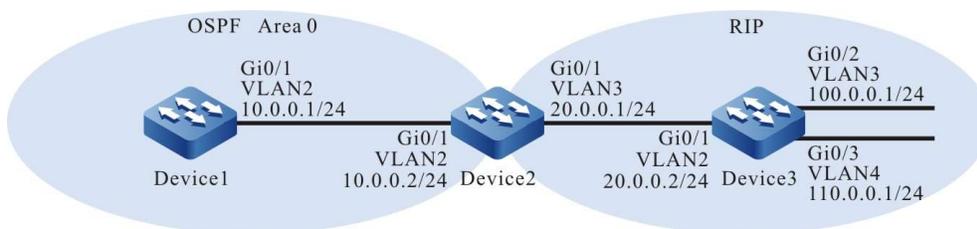


Figure 55-1 Network Topology for Configuring OSPF Route Redistribution

#### Configuration Steps

- Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)
- Step 2: Configures IP addresses for the ports. (Omitted)
- Step 3: Configure the OSPF protocol of Device1 and Device2; configure the RIPv2 protocol of Device2 and Device3.

#Configure the OSPF protocol of Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#router-id 1.1.1.1
Device1(config-ospf)#network 10.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#exit
```

#### #Configure the OSPF and RIPv2 protocols of Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#router-id 2.2.2.2
Device2(config-ospf)#network 10.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#exit
Device2(config)#router rip
Device2(config-rip)#version 2
Device2(config-rip)#network 20.0.0.0
Device2(config-rip)#exit
```

#### #Configure the RIPv2 protocol of Device3.

```
Device3#configure terminal
Device3(config)#router rip
Device3(config-rip)#version 2
Device3(config-rip)#network 20.0.0.0
Device3(config-rip)#network 100.0.0.0
Device3(config-rip)#network 110.0.0.0
Device3(config-rip)#exit
```

#### #View the information of OSPF neighbors on Device1.

```
Device1#show ip ospf neighbor
OSPF process 100:
Neighbor ID  Pri  State      Dead Time  Address      Interface
2.2.2.2      1  Full/DR    00:00:32  10.0.0.2    vlan2
```

#### #View the information of OSPF neighbors on Device2.

```
Device2#show ip ospf neighbor
OSPF process 100:
Neighbor ID  Pri  State      Dead Time  Address      Interface
1.1.1.1      1  Full/Backup 00:00:32  10.0.0.1    vlan2
```

#### #View the routing table of Device 2.

```
Device2#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 10.0.0.0/24 is directly connected, 00:21:17, vlan2
C 20.0.0.0/24 is directly connected, 00:21:33, vlan3
R 100.0.0.0/24 [120/1] via 20.0.0.2, 00:10:58, vlan3
R 110.0.0.0/24 [120/1] via 20.0.0.2, 00:10:58, vlan3
C 127.0.0.0/8 is directly connected, 30:20:17, lo0
```

Device2 learns RIP routes.

#### Step 4: Configure routing policy.

#### #Configure Device2.

```
Device2(config)#ip access-list standard 1
Device2(config-std-nacl)#permit 100.0.0.0 0.0.0.255
Device2(config-std-nacl)#exit
Device2(config)#route-map RIPtoOSPF
Device2(config-route-map)#match ip address 1
Device2(config-route-map)#exit
```

Configure route-map to invoke ACL to match 100.0.0.0/24 only, and filter other network segments, such as 20.0.0.0/24 and 110.0.0.0/24.

Step 5: Configure OSPF to redistribute RIP routes and associate routing policy.

#Configure Device2.

```
Device2(config)#router ospf 100
Device2(config-ospf)#redistribute rip route-map RIPtoOSPF
Device2(config-ospf)#exit
```

When redistributing RIP routes, invoke the match rules of route-map for filtration.

Step 6: Check the result.

#View the routing table of Device1.

```
Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 10.0.0.0/24 is directly connected, 00:47:27, vlan2
OE 100.0.0.0/24 [150/20] via 10.0.0.2, 00:21:39, vlan2
C 127.0.0.0/8 is directly connected, 21:40:06, lo0
```

The routing table of Device1 only learns 100.0.0.0/24, an OSPF external route. The two routes 20.0.0.0/24 and 110.0.0.0/24 are filtered out.

#View the information of OSPF process and database on Device2.

```
Device2#show ip ospf 100
Routing Process "ospf 100" with ID 2.2.2.2
Process bound to VRF default
Process uptime is 1 hour 4 minutes
IETF NSF restarter support disabled
IETF NSF helper support enabled
Conforms to RFC2328, and RFC1583Compatibility flag is disabled
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Graceful Restart
This router is an ASBR (injecting external routing information)
Initial SPF schedule delay 5000 msec
Minimum hold time between two consecutive SPF's 10000 msec
Maximum wait time between two consecutive SPF's 10000 msec
Refresh timer 10 secs
Number of external LSA 2. Checksum Sum 0x0161F5
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of non-default external LSA is 2
External LSA database is unlimited.
Not Support Demand Circuit lsa number is 0, autonomy system support flood DoNotAge Lsa
Number of areas attached to this router: 1
Area 0 (BACKBONE) Number of interfaces in this area is 1(1)
Number of fully adjacent neighbors in this area is 1
Number of fully adjacent sham-link neighbors in this area is 0
Area has no authentication
SPF algorithm last executed 00:37:52.833 ago
SPF algorithm executed 3 times
Number of LSA 3. Checksum Sum 0x00e746
Not Support Demand Circuit lsa number is 0,
Indication lsa (by other routers) number is: 0,
Area support flood DoNotAge Lsa

Device2#show ip ospf 100 database
```

OSPF Router with ID (2.2.2.2) (Process ID 100)

Router Link States (Area 0)

Link ID	ADV Router	Age	Seq#	CkSum	Link count
1.1.1.1	1.1.1.1	191	0x80000004	0x70a0	1
2.2.2.2	2.2.2.2	537	0x80000005	0x36ce	1

Net Link States (Area 0)

Link ID	ADV Router	Age	Seq#	CkSum
10.0.0.2	2.2.2.2	818	0x80000003	0x3fd8

AS External Link States

Link ID	ADV Router	Age	Seq#	CkSum	Route
100.0.0.0	2.2.2.2	718	0x80000002	0x72be	E2 100.0.0.0/24 [0x0]

According to the information of OSPF 100 process, Device2 has become an ASBR, and only an external LSA is generated in the database.

---

## Note

- In practical applications, if the autonomous system has 2 or more edge routers, directly redistributing routes between different routing protocols is not recommended. When necessary, routing policy needs to be configured to avoid routing loops.
- 

### 55.3.4 Configure OSPF multiprocess

#### Network Requirements

- All devices run OSPF protocol. Two OSPF processes are enabled on Device2. Neighbors are established between the OSPF 100 processes of Device1 and Device2, and between the OSPF 200 processes of Device3 and Device2.
- The two OSPF processes on Device2 redistribute routes to each other. OSPF 100 process uses routing policy control to redistribute the route 110.0.0.0/24 only; OSPF 200 process uses routing policy control to redistribute the route 100.0.0.0/24 only.

#### Network Topology

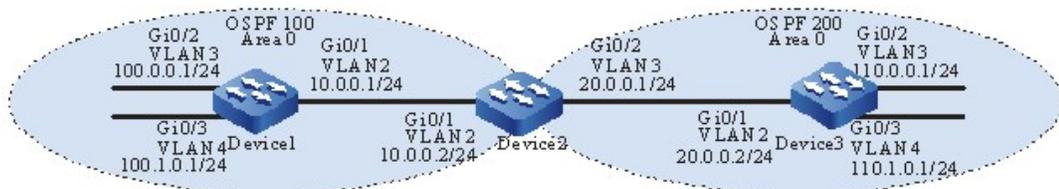


Figure 55-4 Network Topology for Configuring OSPF Multiprocess

## Configuration Steps

Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configures IP addresses for the ports. (Omitted)

Step 3: Configure OSPF protocol.

### #Configure Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#router-id 1.1.1.1
Device1(config-ospf)#network 10.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 100.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 100.1.0.0 0.0.0.255 area 0
Device1(config-ospf)#exit
```

### #On Device2, create 2 OSPF processes, i.e. process 100 and process 200.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#router-id 2.2.2.2
Device2(config-ospf)#network 10.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#exit
Device2(config)#router ospf 200
Device2(config-ospf)#router-id 2.2.2.3
Device2(config-ospf)#network 20.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#exit
```

### #Configure Device3.

```
Device3#configure terminal
Device3(config)#router ospf 200
Device3(config-ospf)#router-id 3.3.3.3
Device3(config-ospf)#network 20.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 110.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 110.1.0.0 0.0.0.255 area 0
Device3(config-ospf)#exit
```

---

## Note

- When there are multiple OSPF processes, it is recommended to configure different Router IDs between OSPF processes to avoid Router ID conflict.
- 

### #View the information of LSDB and neighbors on Device2.

```
Device2#show ip ospf neighbor
OSPF process 100:
Neighbor ID  Pri  State      Dead Time  Address    Interface
1.1.1.1      1  Full/Backup  00:00:30  10.0.0.1  vlan2
OSPF process 200:
Neighbor ID  Pri  State      Dead Time  Address    Interface
3.3.3.3      1  Full/DR     00:00:33  20.0.0.2  vlan3
```

```
Device2#show ip ospf database
```

```
OSPF Router with ID (2.2.2.2) (Process ID 100)
```

```
Router Link States (Area 0)
```

Link ID	ADV Router	Age	Seq#	CkSum	Link count
1.1.1.1	1.1.1.1	19	0x80000016	0x53bf	3
2.2.2.2	2.2.2.2	15	0x80000010	0x1ae1	1

```
Net Link States (Area 0)
```

Link ID	ADV Router	Age	Seq#	CkSum
10.0.0.2	2.2.2.2	21	0x80000001	0x43d6

```
OSPF Router with ID (2.2.2.3) (Process ID 200)
```

```
Router Link States (Area 0)
```

Link ID	ADV Router	Age	Seq#	CkSum	Link count
2.2.2.3	2.2.2.3	14	0x8000000f	0xb235	1
3.3.3.3	3.3.3.3	15	0x8000001b	0x696b	3

```
Net Link States (Area 0)
```

Link ID	ADV Router	Age	Seq#	CkSum
20.0.0.2	3.3.3.3	15	0x80000002	0x03fe

On Device2 which owns the OSPF database by itself, the OSPF process 100 establishes neighbor relation with the process 200.

#View the OSPF routing table of Device2.

```
Device2#show ip ospf route
```

```
OSPF process 100:
```

```
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area  
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2  
E1 - OSPF external type 1, E2 - OSPF external type 2
```

```
O 10.0.0.0/24 [1] is directly connected, vlan2, Area 0  
O 100.0.0.0/24 [2] via 10.0.0.1, vlan2, Area 0  
O 100.1.0.0/24 [2] via 10.0.0.1, vlan2, Area 0
```

```
OSPF process 200:
```

```
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area  
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2  
E1 - OSPF external type 1, E2 - OSPF external type 2
```

```
O 20.0.0.0/24 [1] is directly connected, vlan3, Area 0  
O 110.0.0.0/24 [2] via 20.0.0.2, vlan3, Area 0  
O 110.1.0.0/24 [2] via 20.0.0.2, vlan3, Area 0
```

The OSPF process 100 and 200 calculate their respective routes.

#View the routing table of Device 2.

```
Device2#show ip route
```

```
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
```

```
U - Per-user Static route
```

```
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
C 10.0.0.0/24 is directly connected, 00:05:34, vlan2  
C 20.0.0.0/24 is directly connected, 00:05:28, vlan3  
O 100.0.0.0/24 [110/2] via 10.0.0.1, 00:04:42, vlan2  
O 100.1.0.0/24 [110/2] via 10.0.0.1, 00:04:42, vlan2  
O 110.0.0.0/24 [110/2] via 20.0.0.2, 00:04:41, vlan3  
O 110.1.0.0/24 [110/2] via 20.0.0.2, 00:04:41, vlan3  
C 127.0.0.0/8 is directly connected, 48:40:33, lo0
```

Step 4: Configure routing policy.

#Configure Device2.

```
Device2(config)#ip prefix-list 1 permit 110.0.0.0/24
Device2(config)#ip prefix-list 2 permit 100.0.0.0/24
Device2(config)#route-map OSPF200to100
Device2(config-route-map)#match ip address prefix-list 1
Device2(config-route-map)#exit
Device2(config)#route-map OSPF100to200
Device2(config-route-map)#match ip address prefix-list 2
Device2(config-route-map)#exit
```

Configure route-map to invoke prefix list 1 and 2 to match the network segment 110.0.0.0/24 and 100.0.0.0/24.

---

 **Note**

- When configuring a routing policy, both the prefix list and ACL can create filtering rules. The difference is that the prefix list can accurately match the routing mask.
- 

Step 5: Configure to redistribute routes between OSPF processes and associate routing policy.

#Configure Device2.

```
Device2(config)#router ospf 100
Device2(config-ospf)#redistribute ospf 200 route-map OSPF200to100
Device2(config-ospf)#exit
Device2(config)#router ospf 200
Device2(config-ospf)#redistribute ospf 100 route-map OSPF100to200
Device2(config-ospf)#exit
```

Step 6: Check the result.

#View the OSPF LSDB of Device2.

```
Device2#show ip ospf database

      OSPF Router with ID (2.2.2.2) (Process ID 100)

      Router Link States (Area 0)

Link ID        ADV Router   Age Seq#       CkSum  Link count
1.1.1.1        1.1.1.1     1663 0x80000016 0x53bf3
2.2.2.2        2.2.2.2     216 0x80000011 0x1eda 1

      Net Link States (Area 0)

Link ID        ADV Router   Age Seq#       CkSum
10.0.0.2       2.2.2.2     1664 0x80000001 0x43d6

      AS External Link States
```

```

Link ID    ADV Router  Age Seq#    CkSum Route
110.0.0.0  2.2.2.2    216 0x80000001 0x3dfc E2 110.0.0.0/24 [0x0]

```

OSPF Router with ID (2.2.2.3) (Process ID 200)

Router Link States (Area 0)

```

Link ID    ADV Router  Age Seq#    CkSum Link count
2.2.2.3    2.2.2.3    205 0x80000010 0xb62e 1
3.3.3.3    3.3.3.3    1658 0x8000001b 0x696b 3

```

Net Link States (Area 0)

```

Link ID    ADV Router  Age Seq#    CkSum
20.0.0.2   3.3.3.3    1658 0x80000002 0x03fe

```

AS External Link States

```

Link ID    ADV Router  Age Seq#    CkSum Route
100.0.0.0  2.2.2.3    205 0x80000001 0xb989 E2 100.0.0.0/24 [0x0]

```

It can be seen that the OSPF process 100 has the LSA of 110.0.0.0/24 only, and other routes 110.1.0.0/24 and 20.0.0.0/24 have been filtered out by the routing policy OSPF200to100; the OSPF process 200 has the LSA of 100.0.0.0/24 only, and other routes 100.1.0.0/24 and 10.0.0.0/24 have been filtered out by the routing policy OSPF100to200.

#View the routing table of Device1.

```

Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 10.0.0.0/24 is directly connected, 00:40:20, vlan2
C 100.0.0.0/24 is directly connected, 03:11:36, vlan3
C 100.1.0.0/24 is directly connected, 01:00:22, vlan4
OE 110.0.0.0/24 [150/2] via 10.0.0.2, 00:15:27, vlan2
C 127.0.0.0/8 is directly connected, 97:08:23, lo0

```

Device1 learns the route 110.0.0.0/24 only.

#Check the routing table of Device3.

```

Device3#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 20.0.0.0/24 is directly connected, 00:42:44, vlan2
OE 100.0.0.0/24 [150/2] via 20.0.0.1, 00:17:45, vlan2
C 110.0.0.0/24 is directly connected, 01:02:03, vlan3
C 110.1.0.0/24 is directly connected, 01:02:14, vlan4
C 127.0.0.0/8 is directly connected, 41:02:01, lo0

```

Device3 learns the route 100.0.0.0/24 only.

---

## Note

- In practical applications, if the autonomous system has 2 or more edge routers, directly redistributing routes between different OSPF processes is not recommended. When
-

---

necessary, route filtration policy needs to be configured to avoid routing loops.

---

### 55.3.5 Configure OSPF External Route Summarization

#### Network Requirements

- OSPF protocol is run between Device1 and Device2, and RIPv2 protocol is run between Device2 and Device3.
- Device2 redistributes RIP routes to OSPF. In order to reduce the number of routes on Device1, the RIP routes redistributed on ASBR are summarized as 20.0.0.0/16.

#### Network Topology

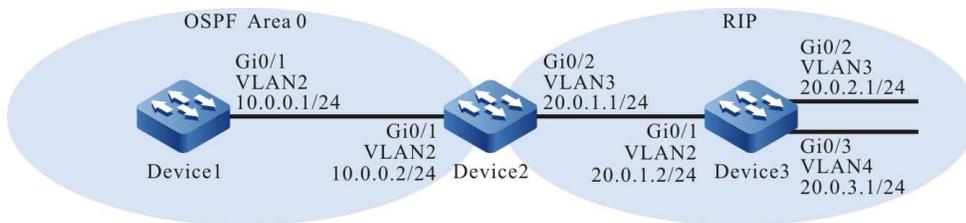


Figure 55-5 Network Topology for Configuring OSPF External Route Summarization

#### Configuration Steps

Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configures IP addresses for the ports. (Omitted)

Step 3: Configure OSPF and RIPv2 protocols.

#Configure the OSPF protocol of Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#router-id 1.1.1.1
Device1(config-ospf)#network 10.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#exit
```

#Configure the OSPF and RIPv2 protocols of Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#router-id 2.2.2.2
Device2(config-ospf)#network 10.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#exit
Device2(config)#router rip
Device2(config-rip)#version 2
Device2(config-rip)#network 20.0.0.0
Device2(config-rip)#exit
```

#Configure the RIPv2 protocol of Device3.

```
Device3#configure terminal
```

```

Device3(config)#router rip
Device3(config-rip)#version 2
Device3(config-rip)#network 20.0.0.0
Device3(config-rip)#exit

```

#### #View the routing table of Device 2.

```

Device2#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
U - Per-user Static route
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 10.0.0.0/24 is directly connected, 00:15:46, vlan2
C 20.0.1.0/24 is directly connected, 00:15:23, vlan3
R 20.0.2.0/24 [120/1] via 20.0.1.2, 00:12:17, vlan3
R 20.0.3.0/24 [120/1] via 20.0.1.2, 00:12:06, vlan3
C 127.0.0.0/8 is directly connected, 03:34:27, lo0

```

#### Step 4: Configure OSPF to redistribute RIP routes.

#### #Configure Device2.

```

Device2(config)#router ospf 100
Device2(config-ospf)#redistribute rip
Device2(config-ospf)#exit

```

#### #View the OSPF LSDB of Device2.

```

Device2#show ip ospf database

OSPF Router with ID (2.2.2.2) (Process ID 100)

Router Link States (Area 0)

Link ID      ADV Router   Age Seq#     CkSum Link count
1.1.1.1      1.1.1.1     1071 0x80000003 0x729f 1
2.2.2.2      2.2.2.2     873 0x80000004 0x38cd 1

Net Link States (Area 0)

Link ID      ADV Router   Age Seq#     CkSum
10.0.0.2     2.2.2.2     1070 0x80000001 0x43d6

AS External Link States

Link ID      ADV Router   Age Seq#     CkSum Route
20.0.1.0     2.2.2.2     365 0x80000001 0x7d04 E2 20.0.1.0/24 [0x0]
20.0.2.0     2.2.2.2     365 0x80000001 0x720e E2 20.0.2.0/24 [0x0]
20.0.3.0     2.2.2.2     365 0x80000001 0x6718 E2 20.0.3.0/24 [0x0]

```

According to the OSPF database, 3 external LSAs have been generated. This indicates that RIP routes have been redistributed to OSPF.

#### #View the routing table of Device1.

```

Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
U - Per-user Static route
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 10.0.0.0/24 is directly connected, 00:56:40, vlan2
OE 20.0.1.0/24 [150/20] via 10.0.0.2, 00:02:40, vlan2
OE 20.0.2.0/24 [150/20] via 10.0.0.2, 00:02:40, vlan2
OE 20.0.3.0/24 [150/20] via 10.0.0.2, 00:02:40, vlan2
C 127.0.0.0/8 is directly connected, 115:12:28, lo0

```

Device1 learns the RIP route redistributed by Device1.

Step 5: OSPF external route summarization is configured on ASBR. At this moment, Device2 acts as an ASBR.

#On Device2, summarize the RIP routes redistributed as 20.0.0.0/16.

```
Device2(config)#router ospf 100
Device2(config-ospf)#summary-address 20.0.0.0 255.255.0.0
Device2(config-ospf)#exit
```

Step 6: Check the result.

#View the OSPF LSDB of Device2.

```
Device2#show ip ospf database

        OSPF Router with ID (2.2.2.2) (Process ID 100)

        Router Link States (Area 0)

Link ID      ADV Router   Age Seq#     CkSum Link count
1.1.1.1     1.1.1.1     1437 0x80000003 0x729f 1
2.2.2.2     2.2.2.2     1240 0x80000004 0x38ed 1

        Net Link States (Area 0)

Link ID      ADV Router   Age Seq#     CkSum
10.0.0.2    2.2.2.2     144 0x80000002 0x41d7

        AS External Link States

Link ID      ADV Router   Age Seq#     CkSum Route
20.0.0.0    2.2.2.2     84 0x80000001 0x88f9 E2 20.0.0.0/16 [0x0]
```

By comparing to step 3, you can see that the original 3 external LSAs in the database have been deleted, and a summarized external LSA is generated.

#View the routing table of Device 2.

```
Device2#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 10.0.0.0/24 is directly connected, 00:28:03, vlan2
O 20.0.0.0/16 [110/1] is directly connected, 00:04:48, null0
C 20.0.1.0/24 is directly connected, 00:27:40, vlan3
R 20.0.2.0/24 [120/1] via 20.0.1.2, 00:24:34, vlan3
R 20.0.3.0/24 [120/1] via 20.0.1.2, 00:24:23, vlan3
C 127.0.0.0/8 is directly connected, 03:46:44, lo0
```

---

## Note

- A summarized route 20.0.0.0/16 which has an output interface pointing to Null0 will be automatically added in the routing table of Device2. This route can prevent loops from
-

---

being produced.

---

#View the routing table of Device1.

```
Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 10.0.0.0/24 is directly connected, 00:58:40, vlan2
OE 20.0.0.0/16 [150/20] via 10.0.0.2, 00:15:26, vlan2
C 127.0.0.0/8 is directly connected, 115:17:28, lo0
```

The routing table of Device1 learns the summarized route 20.0.0.0/16 only.

### 55.3.6 Configure OSPF Inter-area Summarization

#### Network Requirements

- All devices are configured with OSPF protocol, and there are two areas, i.e. area 0 and 1.
- In order to reduce the number of inter-area routes, inter-area summarization should be done on ABR to summarize the routes in area 0 as 10.0.0.0/16 and those in area 1 as 20.0.0.0/16.

#### Network Topology

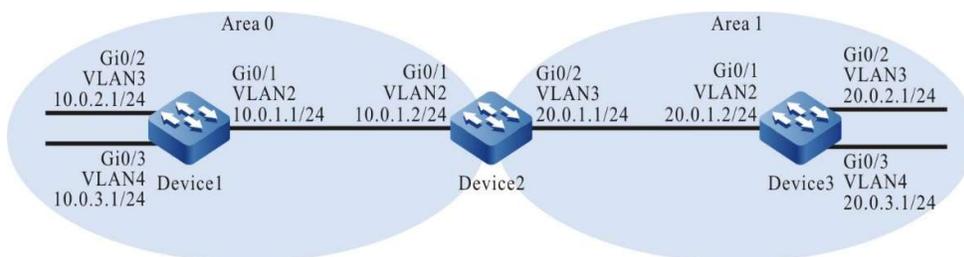


Figure 55-6 Network Topology for Configuring OSPF Inter-area Route Summarization

#### Configuration Steps

- Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)
- Step 2: Configures IP addresses for the ports. (Omitted)
- Step 3: Configure OSPF process and make different areas cover corresponding interfaces.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#router-id 1.1.1.1
Device1(config-ospf)#network 10.0.1.0 0.0.0.255 area 0
Device1(config-ospf)#network 10.0.2.0 0.0.0.255 area 0
```

```
Device1(config-ospf)#network 10.0.3.0 0.0.0.255 area 0
Device1(config-ospf)#exit
```

### #Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#router-id 2.2.2.2
Device2(config-ospf)#network 10.0.1.0 0.0.0.255 area 0
Device2(config-ospf)#network 20.0.1.0 0.0.0.255 area 1
Device2(config-ospf)#exit
```

### #Configure Device3.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#router-id 3.3.3.3
Device3(config-ospf)#network 20.0.1.0 0.0.0.255 area 1
Device3(config-ospf)#network 20.0.2.0 0.0.0.255 area 1
Device3(config-ospf)#network 20.0.3.0 0.0.0.255 area 1
Device3(config-ospf)#exit
```

### #View the OSPF LSDB and routing table on Device2.

```
Device2#show ip ospf database
```

OSPF Router with ID (2.2.2.2) (Process ID 100)

#### Router Link States (Area 0)

Link ID	ADV Router	Age	Seq#	CkSum	Link count
1.1.1.1	1.1.1.1	1419	0x80000007	0x4f81	3
2.2.2.2	2.2.2.2	1414	0x80000004	0x4bb9	1

#### Net Link States (Area 0)

Link ID	ADV Router	Age	Seq#	CkSum
10.0.1.2	2.2.2.2	1419	0x80000001	0x38e0

#### Summary Link States (Area 0)

Link ID	ADV Router	Age	Seq#	CkSum	Route
20.0.1.0	2.2.2.2	1437	0x80000001	0x47d7	20.0.1.0/24
20.0.2.0	2.2.2.2	1363	0x80000001	0x46d6	20.0.2.0/24
20.0.3.0	2.2.2.2	1363	0x80000001	0x3be0	20.0.3.0/24

#### Router Link States (Area 1)

Link ID	ADV Router	Age	Seq#	CkSum	Link count
2.2.2.2	2.2.2.2	1368	0x80000004	0xe70b	1
3.3.3.3	3.3.3.3	1341	0x80000006	0x6138	3

#### Net Link States (Area 1)

Link ID	ADV Router	Age	Seq#	CkSum
20.0.1.1	2.2.2.2	1368	0x80000001	0x24e3

#### Summary Link States (Area 1)

Link ID	ADV Router	Age	Seq#	CkSum	Route
10.0.1.0	2.2.2.2	1442	0x80000001	0xc95f	10.0.1.0/24
10.0.2.0	2.2.2.2	1409	0x80000001	0xc85e	10.0.2.0/24
10.0.3.0	2.2.2.2	1409	0x80000001	0xbd68	10.0.3.0/24

```
Device2#show ip route
```

Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS

U - Per-user Static route

O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

```
C 10.0.1.0/24 is directly connected, 00:30:31, vlan2
```

```

O 10.0.2.0/24 [110/2] via 10.0.1.1, 00:23:37, vlan2
O 10.0.3.0/24 [110/2] via 10.0.1.1, 00:23:37, vlan2
C 20.0.1.0/24 is directly connected, 02:09:10, vlan3
O 20.0.2.0/24 [110/2] via 20.0.1.2, 00:22:51, vlan3
O 20.0.3.0/24 [110/2] via 20.0.1.2, 00:22:51, vlan3
C 127.0.0.0/8 is directly connected, 05:28:14, lo0

```

3 inter-area LSAs are generated in area 0 and 1 of OSPF database on Device2. The intra-area routes in each area are also added to the routing table.

#View the OSPF LSDB and routing table on Device1.

```

Device1#show ip ospf database

      OSPF Router with ID (1.1.1.1) (Process ID 100)

      Router Link States (Area 0)

Link ID      ADV Router   Age Seq#     CkSum Link count
1.1.1.1      1.1.1.1      249 0x80000008 0x4d82 3
2.2.2.2      2.2.2.2      191 0x80000005 0x49ba 1

      Net Link States (Area 0)

Link ID      ADV Router   Age Seq#     CkSum
10.0.1.2     2.2.2.2      471 0x80000002 0x36e1

      Summary Link States (Area 0)

Link ID      ADV Router   Age Seq#     CkSum Route
20.0.1.0     2.2.2.2      251 0x80000002 0x45d8 20.0.1.0/24
20.0.2.0     2.2.2.2      1988 0x80000001 0x46d6 20.0.2.0/24
20.0.3.0     2.2.2.2      1988 0x80000001 0x3be0 20.0.3.0/24

Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 10.0.1.0/24 is directly connected, 00:25:11, vlan2
C 10.0.2.0/24 is directly connected, 00:24:58, vlan3
C 10.0.3.0/24 is directly connected, 00:24:44, vlan4
O 20.0.1.0/24 [110/2] via 10.0.1.2, 00:14:59, vlan2
O 20.0.2.0/24 [110/3] via 10.0.1.2, 00:14:12, vlan2
O 20.0.3.0/24 [110/3] via 10.0.1.2, 00:14:12, vlan2
C 127.0.0.0/8 is directly connected, 116:19:42, lo0

```

There are 3 inter-area LSAs in the OSPF database of Device1, which are also added to the routing table.

#View the OSPF LSDB and routing table on Device3.

```

Device3#show ip ospf database

      OSPF Router with ID (3.3.3.3) (Process ID 100)

      Router Link States (Area 1)

Link ID      ADV Router   Age Seq#     CkSum Link count
2.2.2.2      2.2.2.2      532 0x80000005 0xe50c 1
3.3.3.3      3.3.3.3      506 0x80000007 0x5f39 3

      Net Link States (Area 1)

Link ID      ADV Router   Age Seq#     CkSum
20.0.1.1     2.2.2.2      532 0x80000002 0x22e4

      Summary Link States (Area 1)

Link ID      ADV Router   Age Seq#     CkSum Route

```

```

10.0.1.0 2.2.2.2 82 0x80000002 0xc760 10.0.1.0/24
10.0.2.0 2.2.2.2 382 0x80000002 0xc65f 10.0.2.0/24
10.0.3.0 2.2.2.2 262 0x80000002 0xbb69 10.0.3.0/24

```

```

Device3#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

```

```

O 10.0.1.0/24 [110/2] via 20.0.1.1, 00:24:04, vlan2
O 10.0.2.0/24 [110/3] via 20.0.1.1, 00:24:04, vlan2
O 10.0.3.0/24 [110/3] via 20.0.1.1, 00:24:04, vlan2
C 20.0.1.0/24 is directly connected, 02:09:51, vlan2
C 20.0.2.0/24 is directly connected, 02:07:21, vlan3
C 20.0.3.0/24 is directly connected, 02:07:09, vlan4
C 127.0.0.0/8 is directly connected, 360:20:45, lo0

```

Likewise, there are 3 inter-area LSAs in the OSPF database of Device3, which are also added to the routing table.

Step 4: Inter-area route summarization is configured on ASBR. At this moment, Device2 acts as an ABR.

#On Device2, summarize the routes in area 0 as 10.0.0.0/16 and those in area 1 as 20.0.0.0/16.

```

Device2(config)#router ospf 100
Device2(config-ospf)#area 0 range 10.0.0.0/16
Device2(config-ospf)#area 1 range 20.0.0.0/16
Device2(config-ospf)#exit

```

Step 5: Check the result.

#View the OSPF LSDB and routing table on Device2.

```

Device2#show ip ospf database

        OSPF Router with ID (2.2.2.2) (Process ID 100)

        Router Link States (Area 0)

Link ID    ADV Router   Age Seq#    CkSum Link count
1.1.1.1    1.1.1.1     305 0x80000009 0x4b83 3
2.2.2.2    2.2.2.2     297 0x80000006 0x47bb 1

        Net Link States (Area 0)

Link ID    ADV Router   Age Seq#    CkSum
10.0.1.2   2.2.2.2     527 0x80000003 0x34e2

        Summary Link States (Area 0)

Link ID    ADV Router   Age Seq#    CkSum Route
20.0.0.0   2.2.2.2     23 0x80000001 0x52cd 20.0.0.0/16

        Router Link States (Area 1)

Link ID    ADV Router   Age Seq#    CkSum Link count
2.2.2.2    2.2.2.2     277 0x80000006 0xe30d 1
3.3.3.3    3.3.3.3     332 0x80000008 0x5d3a 3

        Net Link States (Area 1)

Link ID    ADV Router   Age Seq#    CkSum

```

```
20.0.1.1    2.2.2.2    317 0x80000003 0x20e5
```

```
Summary Link States (Area 1)
```

```
Link ID    ADV Router  Age Seq#    CkSum Route
10.0.0.0   2.2.2.2    26 0x80000001 0xd455 10.0.0.0/16
```

```
Device2#show ip route
```

```
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
```

```
U - Per-user Static route
```

```
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
O 10.0.0.0/16 [110/1] is directly connected, 00:00:31, null0
C 10.0.1.0/24 is directly connected, 00:40:31, vlan2
O 10.0.2.0/24 [110/2] via 10.0.1.1, 00:33:37, vlan2
O 10.0.3.0/24 [110/2] via 10.0.1.1, 00:33:37, vlan2
O 20.0.0.0/16 [110/1] is directly connected, 00:00:27, null0
C 20.0.1.0/24 is directly connected, 02:19:10, vlan3
O 20.0.2.0/24 [110/2] via 20.0.1.2, 00:32:51, vlan3
O 20.0.3.0/24 [110/2] via 20.0.1.2, 00:32:51, vlan3
C 127.0.0.0/8 is directly connected, 05:38:14, lo0
```

By comparing to step 2, you can see that a summarized inter-area LSA is generated in area 0 and 1 of OSPF database on Device2. Likewise, a summarized route pointing to Null0 interface will be automatically added to the routing table.

#View the OSPF LSDB and routing table on Device1.

```
Device1#show ip ospf database
```

```
OSPF Router with ID (1.1.1.1) (Process ID 100)
```

```
Router Link States (Area 0)
```

```
Link ID    ADV Router  Age Seq#    CkSum Link count
1.1.1.1    1.1.1.1    1338 0x80000009 0x4b83 3
2.2.2.2    2.2.2.2    1332 0x80000006 0x47bb 1
```

```
Net Link States (Area 0)
```

```
Link ID    ADV Router  Age Seq#    CkSum
10.0.1.2   2.2.2.2    1563 0x80000003 0x34e2
```

```
Summary Link States (Area 0)
```

```
Link ID    ADV Router  Age Seq#    CkSum Route
20.0.0.0   2.2.2.2    90 0x80000001 0x52cd 20.0.0.0/16
```

```
Device1#show ip route
```

```
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
```

```
U - Per-user Static route
```

```
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
C 10.0.1.0/24 is directly connected, 00:40:11, vlan2
C 10.0.2.0/24 is directly connected, 00:39:58, vlan3
C 10.0.3.0/24 is directly connected, 00:39:44, vlan4
O 20.0.0.0/16 [110/2] via 10.0.1.2, 00:02:18, vlan2
C 127.0.0.0/8 is directly connected, 116:44:42, lo0
```

According to the Device1, there is summarized inter-area LSA only in the OSPF database, and the routing table can only learn the route 20.0.0.0/16 summarized in area 1; Device3 can also learn the route 10.0.0.0/16 summarized in area 0.

## 55.3.7 Configure OSPF Inter-area Route Filtration

### Network Requirements

- All devices are configured with OSPF protocol, and there are two areas, i.e. area 0 and 1.
- Filter inter-area routes on ABR. The route 20.0.3.0/24 is not allowed to be injected into area 0, and the route 10.0.3.0/24 is not allowed to flood to other areas.

### Network Topology

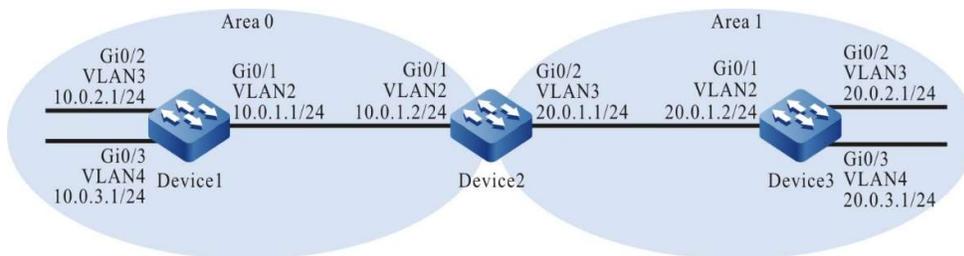


Figure 55-7 Network Topology for Configuring Filtration of OSPF Inter-area Routes

### Configuration Steps

- Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)
- Step 2: Configures IP addresses for the ports. (Omitted)
- Step 3: Configure OSPF process and make different areas cover corresponding interfaces.

#### #Configure Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#router-id 1.1.1.1
Device1(config-ospf)#network 10.0.1.0 0.0.0.255 area 0
Device1(config-ospf)#network 10.0.2.0 0.0.0.255 area 0
Device1(config-ospf)#network 10.0.3.0 0.0.0.255 area 0
Device1(config-ospf)#exit
```

#### #Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#router-id 2.2.2.2
Device2(config-ospf)#network 10.0.1.0 0.0.0.255 area 0
Device2(config-ospf)#network 20.0.1.0 0.0.0.255 area 1
Device2(config-ospf)#exit
```

#### #Configure Device3.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#router-id 3.3.3.3
Device3(config-ospf)#network 20.0.1.0 0.0.0.255 area 1
Device3(config-ospf)#network 20.0.2.0 0.0.0.255 area 1
Device3(config-ospf)#network 20.0.3.0 0.0.0.255 area 1
```

```
Device3(config-ospf)#exit
```

## #View the OSPF LSDB and routing table on Device2.

```
Device2#show ip ospf database
```

```
OSPF Router with ID (2.2.2.2) (Process ID 100)
```

```
Router Link States (Area 0)
```

Link ID	ADV Router	Age	Seq#	CkSum	Link count
1.1.1.1	1.1.1.1	329	0x8000005b	0xa6d5	3
2.2.2.2	2.2.2.2	324	0x80000051	0xb007	1

```
Net Link States (Area 0)
```

Link ID	ADV Router	Age	Seq#	CkSum
10.0.1.2	2.2.2.2	324	0x8000004e	0x9d2e

```
Summary Link States (Area 0)
```

Link ID	ADV Router	Age	Seq#	CkSum	Route
20.0.1.0	2.2.2.2	324	0x8000004e	0xac25	20.0.1.0/24
20.0.2.0	2.2.2.2	324	0x8000004d	0xad23	20.0.2.0/24
20.0.3.0	2.2.2.2	259	0x80000001	0x3be0	20.0.3.0/24

```
Router Link States (Area 1)
```

Link ID	ADV Router	Age	Seq#	CkSum	Link count
2.2.2.2	2.2.2.2	334	0x80000055	0x4f51	1
3.3.3.3	3.3.3.3	335	0x80000059	0xca7a	3

```
Net Link States (Area 1)
```

Link ID	ADV Router	Age	Seq#	CkSum
20.0.1.2	3.3.3.3	340	0x80000001	0xeb17

```
Summary Link States (Area 1)
```

Link ID	ADV Router	Age	Seq#	CkSum	Route
10.0.1.0	2.2.2.2	365	0x80000001	0xc95f	10.0.1.0/24
10.0.2.0	2.2.2.2	319	0x80000001	0xc85e	10.0.2.0/24
10.0.3.0	2.2.2.2	256	0x80000001	0xbd68	10.0.3.0/24

```
Device2#show ip route
```

```
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
```

```
U - Per-user Static route
```

```
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
C 10.0.1.0/24 is directly connected, 00:06:13, vlan2
```

```
O 10.0.2.0/24 [110/2] via 10.0.1.1, 00:05:22, vlan2
```

```
O 10.0.3.0/24 [110/2] via 10.0.1.1, 00:05:22, vlan2
```

```
C 20.0.1.0/24 is directly connected, 00:06:19, vlan3
```

```
O 20.0.2.0/24 [110/2] via 20.0.1.2, 00:05:32, vlan3
```

```
O 20.0.3.0/24 [110/2] via 20.0.1.2, 00:05:32, vlan3
```

```
C 127.0.0.0/8 is directly connected, 94:42:22, lo0
```

3 inter-area LSAs are generated in area 0 and 1 of OSPF database on Device2. The routes in each area are also added to the routing table.

## #View the routing table of Device1.

```
Device1#show ip route
```

```
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
```

```
U - Per-user Static route
```

```
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
C 10.0.1.0/24 is directly connected, 00:08:41, vlan2
```

```
C 10.0.2.0/24 is directly connected, 37:59:10, vlan3
```

```

C 10.0.3.0/24 is directly connected, 38:05:36, vlan4
O 20.0.1.0/24 [110/2] via 10.0.1.2, 00:07:55, vlan2
O 20.0.2.0/24 [110/3] via 10.0.1.2, 00:07:55, vlan2
O 20.0.3.0/24 [110/3] via 10.0.1.2, 00:06:50, vlan2
C 127.0.0.0/8 is directly connected, 70:07:32, lo0

```

Device1 learns the routes in area 1 only.

#Check the routing table of Device3.

```

Device3#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

O 10.0.1.0/24 [110/2] via 20.0.1.1, 00:08:44, vlan2
O 10.0.2.0/24 [110/3] via 20.0.1.1, 00:08:33, vlan2
O 10.0.3.0/24 [110/3] via 20.0.1.1, 00:07:30, vlan2
C 20.0.1.0/24 is directly connected, 00:09:31, vlan2
C 20.0.2.0/24 is directly connected, 37:59:57, vlan3
C 20.0.3.0/24 is directly connected, 38:03:35, vlan4
C 127.0.0.0/8 is directly connected, 61:26:38, lo0

```

Device3 learns the routes in area 0 only.

Step 4: Configure route filtration policy.

#Configure Device2.

```

Device2(config)#ip prefix-list 1 deny 10.0.3.0/24
Device2(config)#ip prefix-list 1 permit 0.0.0.0/0 le 32
Device2(config)#ip prefix-list 2 deny 20.0.3.0/24
Device2(config)#ip prefix-list 2 permit 0.0.0.0/0 le 32
Device2(config)#exit

```

Prefix list 1 means to filter the network 10.0.3.0/24 and allow all the other networks; 2 means to filter the network 20.0.3.0/24 and allow all the other networks.

Step 5: Configure inter-area route filtration on ASBR, and invoke the match rules of prefix list.

#Configure Device2.

```

Device2(config)#router ospf 100
Device2(config-ospf)#area 0 filter-list prefix 1 out
Device2(config-ospf)#area 0 filter-list prefix 2 in
Device2(config-ospf)#exit

```

Step 6: Check the result.

#View the OSPF LSDB of Device2.

```

Device2#show ip ospf database

OSPF Router with ID (2.2.2.2) (Process ID 100)

Router Link States (Area 0)

Link ID      ADV Router   Age Seq#      CkSum Link count
1.1.1.1      1.1.1.1     679 0x8000005b 0xa6d5 3
2.2.2.2      2.2.2.2     673 0x80000051 0xb007 1

```

Net Link States (Area 0)

Link ID	ADV Router	Age	Seq#	CkSum
10.0.1.2	2.2.2.2	673	0x8000004e	0x9d2e

Summary Link States (Area 0)

Link ID	ADV Router	Age	Seq#	CkSum	Route
20.0.1.0	2.2.2.2	673	0x8000004e	0xac25	20.0.1.0/24
20.0.2.0	2.2.2.2	673	0x8000004d	0xad23	20.0.2.0/24

Router Link States (Area 1)

Link ID	ADV Router	Age	Seq#	CkSum	Link count
2.2.2.2	2.2.2.2	683	0x80000055	0x4f51	1
3.3.3.3	3.3.3.3	684	0x80000059	0xca7a	3

Net Link States (Area 1)

Link ID	ADV Router	Age	Seq#	CkSum
20.0.1.2	3.3.3.3	689	0x80000001	0xeb17

Summary Link States (Area 1)

Link ID	ADV Router	Age	Seq#	CkSum	Route
10.0.1.0	2.2.2.2	714	0x80000001	0xc95f	10.0.1.0/24
10.0.2.0	2.2.2.2	668	0x80000001	0xc85e	10.0.2.0/24

By comparing to the result of step 2, you can see that the LSAs of the networks 20.0.3.0/24 and 10.0.3.0/24 in OSPF database have been deleted from area 0 and 1.

#View the routing table of Device1.

```
Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i - ISIS
U - Per-user Static route
O - OSPF, OE - OSPF External, M - Management, E - IRMP, EX - IRMP external

C 10.0.1.0/24 is directly connected, 00:12:57, vlan2
C 10.0.2.0/24 is directly connected, 38:03:25, vlan3
C 10.0.3.0/24 is directly connected, 38:09:52, vlan4
O 20.0.1.0/24 [110/2] via 10.0.1.2, 00:12:11, vlan2
O 20.0.2.0/24 [110/3] via 10.0.1.2, 00:12:11, vlan2
C 127.0.0.0/8 is directly connected, 70:11:48, lo0
```

There has been no 20.0.3.0/24 in the routing table of Device1.

#Check the routing table of Device3.

```
Device3#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i - ISIS
U - Per-user Static route
O - OSPF, OE - OSPF External, M - Management, E - IRMP, EX - IRMP external

O 10.0.1.0/24 [110/2] via 20.0.1.1, 00:13:09, vlan2
O 10.0.2.0/24 [110/3] via 20.0.1.1, 00:12:58, vlan2
C 20.0.1.0/24 is directly connected, 00:13:56, vlan2
C 20.0.2.0/24 is directly connected, 38:04:22, vlan3
C 20.0.3.0/24 is directly connected, 38:08:00, vlan4
C 127.0.0.0/8 is directly connected, 64:31:03, lo0
```

There has been no 10.0.3.0/24 in the routing table of Device3 either.

## 55.3.8 Configure OSPF totally Stub area

### Network Requirements

- All devices are configured with OSPF protocol, and there are three areas, i.e. area 0, 1 and 2. In particular, area 1 is a totally Stub area.
- On Device4, redistribute a static route to OSPF. Upon completion of the configuration, the totally Stub area cannot learn inter-area and external routes, those devices in other areas can learn them.

### Network Topology

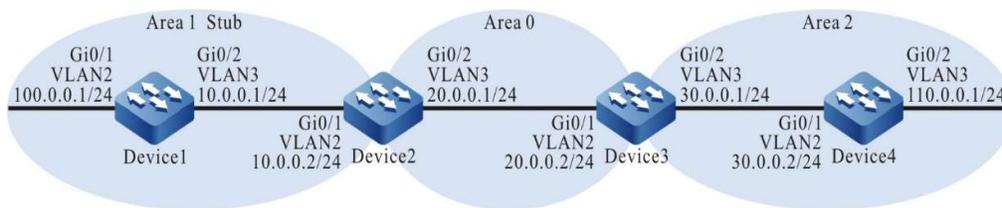


Figure 55-8 Network Topology for Configuring OSPF Totally Stub Area

### Configuration Steps

- Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)
- Step 2: Configures IP addresses for the ports. (Omitted)
- Step 3: Configure OSPF process and make areas cover corresponding interfaces.

#On Device1, configure area 1 as Stub area.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#router-id 1.1.1.1
Device1(config-ospf)#area 1 stub
Device1(config-ospf)#network 10.0.0.0 0.0.0.255 area 1
Device1(config-ospf)#network 100.0.0.0 0.0.0.255 area 1
Device1(config-ospf)#exit
```

#On Device2, configure area 1 as a totally Stub area. Device2 as an ABR. No-summary cannot take effect unless it is configured on ABR.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#router-id 2.2.2.2
Device2(config-ospf)#area 1 stub no-summary
Device2(config-ospf)#network 10.0.0.0 0.0.0.255 area 1
Device2(config-ospf)#network 20.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#exit
```

#Configure Device3.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#router-id 3.3.3.3
```

```
Device3(config-ospf)#network 20.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 30.0.0.0 0.0.0.255 area 2
Device3(config-ospf)#exit
```

#### #Configure Device4.

```
Device4#configure terminal
Device4(config)#router ospf 100
Device4(config-ospf)#router-id 4.4.4.4
Device4(config-ospf)#network 30.0.0.0 0.0.0.255 area 2
Device4(config-ospf)#network 110.0.0.0 0.0.0.255 area 2
Device4(config-ospf)#exit
```

Step 4: Configure a static route for Device4 and redistribute it to OSPF.

#### #Configure Device4.

```
Device4(config)#ip route 200.1.1.0 255.255.255.0 110.0.0.2
Device4(config)#router ospf 100
Device4(config-ospf)#redistribute static
Device4(config-ospf)#exit
```

Step 5: Check the result.

#### #View the OSPF LSDB and routing table on Device1.

```
Device1#show ip ospf database

        OSPF Router with ID (1.1.1.1) (Process ID 100)

        Router Link States (Area 1 [Stub])

Link ID      ADV Router   Age Seq#     CkSum Link count
1.1.1.1      1.1.1.1      19 0x80000009 0x8513 2
2.2.2.2      2.2.2.2      22 0x80000005 0x51b6 1

        Net Link States (Area 1 [Stub])

Link ID      ADV Router   Age Seq#     CkSum
10.0.0.2     2.2.2.2      22 0x80000001 0x61ba

        Summary Link States (Area 1 [Stub])

Link ID      ADV Router   Age Seq#     CkSum Route
0.0.0.0      2.2.2.2      55 0x80000002 0x73c1 0.0.0.0/0

Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

O 0.0.0.0/0 [110/2] via 10.0.0.2, 00:00:19, vlan3
C 10.0.0.0/24 is directly connected, 00:01:04, vlan3
C 100.0.0.0/24 is directly connected, 00:11:55, vlan2
C 127.0.0.0/8 is directly connected, 30:46:57, lo0
```

According to the OSPF database, there are no inter-area LSA or external route LSA except for an inter-area LSA of 0.0.0.0/0 in area 1. The ABR in Stub area will generate an inter-area route of 0.0.0.0/0 which floods in the totally Stub area. The data leading to the outside of area and AS are all forwarded through this default route.

## #View the routing table of Device 2.

```
Device2#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 10.0.0.0/24 is directly connected, 00:01:02, vlan2
C 20.0.0.0/24 is directly connected, 00:00:59, vlan3
O 30.0.0.0/24 [110/2] via 20.0.0.2, 00:00:17, vlan3
O 100.0.0.0/24 [110/2] via 10.0.0.1, 00:00:10, vlan2
O 110.0.0.0/24 [110/3] via 20.0.0.2, 00:00:17, vlan3
C 127.0.0.0/8 is directly connected, 56:07:04, lo0
OE 200.1.1.0/24 [150/20] via 20.0.0.2, 00:00:16, vlan3
```

According to the result, Device2 can learn inter-area routes and external routes.

---

### Note

- When the command **area area-id stub** is configured on the ABR of the Stub area only without adding **no-summary**, the devices in this area can learn inter-area routes instead of external routes, and they still access the network outside the AS through the default route.
- 

## 55.3.9 Configure OSPF NSSA

### Network Requirements

- All devices are configured with OSPF protocol, and there are three areas, i.e. area 0, 1 and 2. In particular, area 1 and 2 are NSSA areas.
- On Device4, redistribute a static route to OSPF. Upon completion of the configuration, all devices can learn intra-area and inter-area routes, yet external routes cannot be injected to area 1.
- Import a default route on the ABR of area 1 so that Device1 can access external network through the default route.

### Network Topology

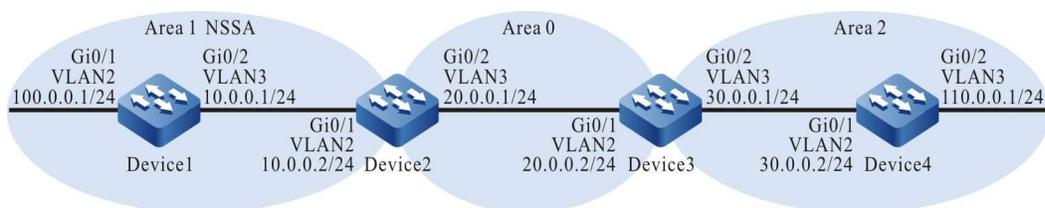


Figure 55-2 Network Topology for Configuring OSPF NSSA Area

### Configuration Steps

Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configures IP addresses for the ports. (Omitted)

Step 3: Configure OSPF process and make areas cover corresponding interfaces.

#On Device1, configure area 1 as NSSA area.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#router-id 1.1.1.1
Device1(config-ospf)#area 1 nssa
Device1(config-ospf)#network 10.0.0.0 0.0.0.255 area 1
Device1(config-ospf)#network 100.0.0.0 0.0.0.255 area 1
Device1(config-ospf)#exit
```

#On Device2, configure area 1 as NSSA area.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#router-id 2.2.2.2
Device2(config-ospf)#area 1 nssa
Device2(config-ospf)#network 10.0.0.0 0.0.0.255 area 1
Device2(config-ospf)#network 20.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#exit
```

#On Device3, configure area 2 as NSSA area.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#router-id 3.3.3.3
Device3(config-ospf)#area 2 nssa
Device3(config-ospf)#network 20.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 30.0.0.0 0.0.0.255 area 2
Device3(config-ospf)#exit
```

#On Device4, configure area 2 as NSSA area.

```
Device4#configure terminal
Device4(config)#router ospf 100
Device4(config-ospf)#router-id 4.4.4.4
Device4(config-ospf)#area 2 nssa
Device4(config-ospf)#network 30.0.0.0 0.0.0.255 area 2
Device4(config-ospf)#network 110.0.0.0 0.0.0.255 area 2
Device4(config-ospf)#exit
```

Step 4: Configure a static route for Device4 and redistribute it to OSPF.

#Configure Device4.

```
Device4(config)#ip route 200.1.1.0 255.255.255.0 110.0.0.2
Device4(config)#router ospf 100
Device4(config-ospf)#redistribute static
Device4(config-ospf)#exit
```

#View the OSPF LSDB of Device3.

```
Device3#show ip ospf database

OSPF Router with ID (3.3.3.3) (Process ID 100)

Router Link States (Area 0)
```

Link ID	ADV Router	Age	Seq#	CkSum	Link count
2.2.2.2	2.2.2.2	179	0x80000004	0xe110	1
3.3.3.3	3.3.3.3	177	0x80000004	0xa345	1

Net Link States (Area 0)

Link ID	ADV Router	Age	Seq#	CkSum
20.0.0.2	3.3.3.3	182	0x80000001	0xf60d

Summary Link States (Area 0)

Link ID	ADV Router	Age	Seq#	CkSum	Route
10.0.0.0	2.2.2.2	214	0x80000001	0xd455	10.0.0.0/24
100.0.0.0	2.2.2.2	173	0x80000001	0x4886	100.0.0.0/24
30.0.0.0	3.3.3.3	208	0x80000001	0xb160	30.0.0.0/24
110.0.0.0	3.3.3.3	171	0x80000001	0xa719	110.0.0.0/24

ASBR-Summary Link States (Area 0)

Link ID	ADV Router	Age	Seq#	CkSum
4.4.4.4	3.3.3.3	171	0x80000001	0x72ac

Router Link States (Area 2 [NSSA])

Link ID	ADV Router	Age	Seq#	CkSum	Link count
3.3.3.3	3.3.3.3	175	0x80000004	0x686f	1
4.4.4.4	4.4.4.4	177	0x80000005	0xe46a	2

Net Link States (Area 2 [NSSA])

Link ID	ADV Router	Age	Seq#	CkSum
30.0.0.2	4.4.4.4	177	0x80000001	0xc827

Summary Link States (Area 2 [NSSA])

Link ID	ADV Router	Age	Seq#	CkSum	Route
10.0.0.0	3.3.3.3	172	0x80000001	0xde48	10.0.0.0/24
20.0.0.0	3.3.3.3	214	0x80000001	0x52cb	20.0.0.0/24
100.0.0.0	3.3.3.3	172	0x80000001	0x5279	100.0.0.0/24

NSSA-external Link States (Area 2 [NSSA])

Link ID	ADV Router	Age	Seq#	CkSum	Route
200.1.1.0	4.4.4.4	247	0x80000001	0x6cde	N2 200.1.1.0/24 [0x0]

AS External Link States

Link ID	ADV Router	Age	Seq#	CkSum	Route
200.1.1.0	3.3.3.3	176	0x80000001	0x0156	E2 200.1.1.0/24 [0x0]

According to the OSPF database, the NSSA-external LSA can be transformed into AS External LSA on the ABR of NSSA area (area 2) so that other areas can normally learn the external routes redistributed from NSSA area (area 2).

#View the routing table of Device 2.

```
Device2#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 10.0.0.0/24 is directly connected, 00:02:53, vlan2
C 20.0.0.0/24 is directly connected, 00:02:51, vlan3
O 30.0.0.0/24 [110/2] via 20.0.0.2, 00:02:04, vlan3
O 100.0.0.0/24 [110/2] via 10.0.0.1, 00:02:04, vlan2
O 110.0.0.0/24 [110/3] via 20.0.0.2, 00:02:02, vlan3
C 127.0.0.0/8 is directly connected, 06:47:22, lo0
```

OE 200.1.1.0/24 [150/20] via 20.0.0.2, 00:02:02, vlan3

Device2 has learned the external routes redistributed from NSSA area (area 2).

#View the routing table of Device1.

```
Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 10.0.0.0/24 is directly connected, 00:02:29, vlan3
O 20.0.0.0/24 [110/2] via 10.0.0.2, 00:01:44, vlan3
O 30.0.0.0/24 [110/3] via 10.0.0.2, 00:01:41, vlan3
C 100.0.0.0/24 is directly connected, 01:53:00, vlan2
O 110.0.0.0/24 [110/4] via 10.0.0.2, 00:01:40, vlan3
C 127.0.0.0/8 is directly connected, 383:45:55, lo0
```

According to the result, there is no 200.1.1.0/24 in the routing table of Device1. This indicates that the external routes redistributed from Device4 are not injected into the NSSA area (area 1), and other inter-area routes have been added into the routing table.

Step 5: Configure Device2 to import default route to area 1.

#Configure Device2 which is the ABR of area 1.

```
Device2(config)#router ospf 100
Device2(config-ospf)#router-id 2.2.2.2
Device2(config-ospf)#area 1 nssa default-information-originate
Device2(config-ospf)#exit
```

---

## Note

- After the command **area area-id nssa no-summary** is configured on the ABR of NSSA area, this area is also called a totally NSSA area. At this moment, ABR also generates a default route and floods to the NSSA area. Configuring this command can further reduce summary LSA and corresponding inter-area routes. Then the networks outside the area and AS are accessed through this default route.
- 

Step 6: Check the result.

#View the OSPF LSDB of Device2.

```
Device2#show ip ospf database

OSPF Router with ID (2.2.2.2) (Process ID 100)

Router Link States (Area 0)

Link ID      ADV Router   Age Seq#     CkSum Link count
2.2.2.2      2.2.2.2     455 0x80000004 0xe110 1
3.3.3.3      3.3.3.3     455 0x80000004 0xa345 1

Net Link States (Area 0)

Link ID      ADV Router   Age Seq#     CkSum
```

```
20.0.0.2 3.3.3.3 461 0x80000001 0xf60d
```

#### Summary Link States (Area 0)

Link ID	ADV Router	Age	Seq#	CkSum	Route
10.0.0.0	2.2.2.2	492	0x80000001	0xd455	10.0.0.0/24
100.0.0.0	2.2.2.2	449	0x80000001	0x4886	100.0.0.0/24
30.0.0.0	3.3.3.3	487	0x80000001	0xb160	30.0.0.0/24
110.0.0.0	3.3.3.3	449	0x80000001	0xa719	110.0.0.0/24

#### ASBR-Summary Link States (Area 0)

Link ID	ADV Router	Age	Seq#	CkSum
4.4.4.4	3.3.3.3	449	0x80000001	0x72ac

#### Router Link States (Area 1 [NSSA])

Link ID	ADV Router	Age	Seq#	CkSum	Link count
1.1.1.1	1.1.1.1	456	0x80000005	0x8d0f	2
2.2.2.2	2.2.2.2	457	0x80000004	0x59ad	1

#### Net Link States (Area 1 [NSSA])

Link ID	ADV Router	Age	Seq#	CkSum
10.0.0.2	2.2.2.2	457	0x80000001	0x61ba

#### Summary Link States (Area 1 [NSSA])

Link ID	ADV Router	Age	Seq#	CkSum	Route
20.0.0.0	2.2.2.2	492	0x80000001	0x70b1	20.0.0.0/24
30.0.0.0	2.2.2.2	449	0x80000001	0xf71f	30.0.0.0/24
110.0.0.0	2.2.2.2	448	0x80000001	0xedd7	110.0.0.0/24

#### NSSA-external Link States (Area 1 [NSSA])

Link ID	ADV Router	Age	Seq#	CkSum	Route
0.0.0.0	2.2.2.2	31	0x80000001	0x5b42	N2 0.0.0.0/0 [0x0]

#### AS External Link States

Link ID	ADV Router	Age	Seq#	CkSum	Route
200.1.1.0	3.3.3.3	454	0x80000001	0x0156	E2 200.1.1.0/24 [0x0]

OSPF generates a NSSA-external LSA for the default route.

#View the routing table of Device1.

```
Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

OE 0.0.0.0/0 [150/1] via 10.0.0.2, 00:00:22, vlan3
C 10.0.0.0/24 is directly connected, 00:07:29, vlan3
O 20.0.0.0/24 [110/2] via 10.0.0.2, 00:06:44, vlan3
O 30.0.0.0/24 [110/3] via 10.0.0.2, 00:06:41, vlan3
C 100.0.0.0/24 is directly connected, 01:58:00, vlan2
O 110.0.0.0/24 [110/4] via 10.0.0.2, 00:06:40, vlan3
C 127.0.0.0/8 is directly connected, 383:50:55, lo0
```

The routing table of Device1 also learns the default route 0.0.0.0/0. The communication with the external routes of AS is achieved through this default route.

## 55.3.10 Configure OSPF to Coordinate with BFD

### Network Requirements

- Configure OSPF protocol for all the devices.
- Enable BFD detection function for the lines between Device1 and Device3. When the lines fail, BFD will quickly identify these failures and notify OSPF which will switch route to Device2 for communication.

### Network Topology

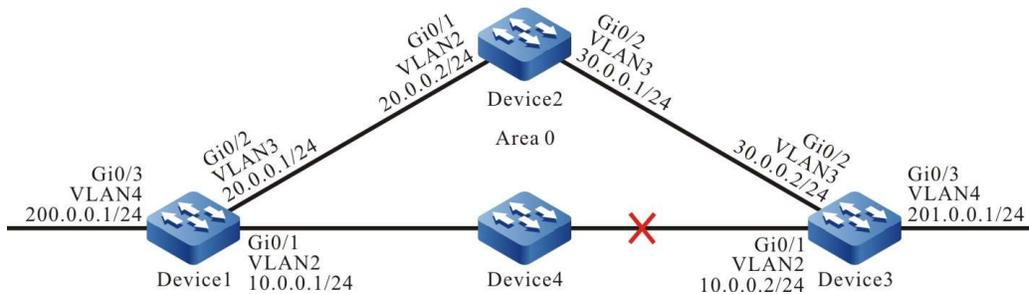


Figure 55-10 Network Topology for Configuring Coordination of OSPF with BFD

### Configuration Steps

- Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)
- Step 2: Configures IP addresses for the ports. (Omitted)
- Step 3: Configure OSPF process.

#### #Configure Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#router-id 1.1.1.1
Device1(config-ospf)#network 10.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 20.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 200.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#exit
```

#### #Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#router-id 2.2.2.2
Device2(config-ospf)#network 20.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#network 30.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#exit
```

#### #Configure Device3.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#router-id 3.3.3.3
Device3(config-ospf)#network 10.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 30.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 201.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#exit
```

Step 4: Configure coordination of OSPF with BFD.

#Configure Device1.

```
Device1(config)#bfd fast-detect
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ip ospf bfd
Device1(config-if-vlan2)#exit
```

#Configure Device3.

```
Device3(config)#bfd fast-detect
Device3(config)#interface vlan2
Device3(config-if-vlan2)#ip ospf bfd
Device3(config-if-vlan2)#exit
```

Step 5: Check the result.

#View OSPF neighbors' information and routing table on Device1.

```
Device1#show ip ospf neighbor 3.3.3.3

OSPF process 100:
Neighbor 3.3.3.3, interface address 10.0.0.2
  In the area 0 via interface vlan2, BFD enabled
  Neighbor priority is 1, State is Full, 5 state changes
  DR is 10.0.0.2, BDR is 10.0.0.1
  Options is 0x42 (-|O|-|E|-)
  Dead timer due in 00:00:31
  Neighbor is up for 00:02:46
  Database Summary List 0
  Link State Request List 0
  Link State Retransmission List 0
  Crypt Sequence Number is 0
  Graceful restart proxy id is 0x0
  Thread Inactivity Timer on
  Thread Database Description Retransmission off, 0 times
  Thread Link State Request Retransmission off, 0 times
  Thread Link State Update Retransmission off, 0 times

Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 10.0.0.0/24 is directly connected, 00:01:09, vlan2
C 20.0.0.0/24 is directly connected, 00:55:37, vlan3
O 30.0.0.0/24 [110/2] via 20.0.0.2, 00:02:50, vlan3
  [110/2] via 10.0.0.2, 00:01:30, vlan2
C 127.0.0.0/8 is directly connected, 05:51:09, lo0
C 200.0.0.0/24 is directly connected, 00:55:12, vlan4
O 201.0.0.0/24 [110/2] via 10.0.0.2, 00:01:30, vlan2
```

According to the information of OSPF neighbors, BFD has been enabled, and the route 201.0.0.0/24 prefers the lines between Device1 and Device3 for communication.

#View the BFD session information of Device1.

```
Device1#show bfd session detail
Total session number: 1
OurAddr      NeighAddr      LD/RD      State      Holddown      interface
10.0.0.1      10.0.0.2      7/14      UP      5000      vlan2
Type:direct
```

```

Local State:UP Remote State:UP Up for: 0h:2m:37s Number of times UP:1
Send Interval:1000ms Detection time:5000ms(1000ms*5)
Local Diag:0 Demand mode:0 Poll bit:0
MinTxInt:1000 MinRxInt:1000 Multiplier:5
Remote MinTxInt:1000 Remote MinRxInt:1000 Remote Multiplier:5
Registered modules:Registered modules:OSPF

```

According to the result, OSPF has been successfully coordinated with BFD, and the session is established normally.

#When the lines between Device1 and Device3 fail, BFD can quickly identify these failures and notify OSPF which will switch route to Device2 for communication and view the routing table on Device1.

```

%BFD-5-Session [10.0.0.2,10.0.0.1,vlan2,10] DOWN (Detection time expired)
%OSPF-5-ADJCHG: Process 100 Nbr [vlan2:10.0.0.1-3.3.3.3] from Full to Down,KillNbr: BFD session down

```

```

Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 10.0.0.0/24 is directly connected, 00:01:59, vlan2
C 20.0.0.0/24 is directly connected, 00:56:13, vlan3
O 30.0.0.0/24 [110/2] via 20.0.0.2, 00:03:40, vlan3
C 127.0.0.0/8 is directly connected, 05:52:41, lo0
C 200.0.0.0/24 is directly connected, 00:56:02, vlan4
O 201.0.0.0/24 [110/3] via 20.0.0.2, 00:00:06, vlan3

```

Device3 has similar behaviors to Device1.

### 55.3.11 Configure OSPF FRR

#### Network Requirements

- Configure OSPF protocol for all the devices.
- Device1 learns the OSPF route 192.168.1.1/32 from Device2 and Device3 at the same time, and first uses the lines between it and Device3 to forward packets. Likewise, Device3 learns the OSPF route 100.1.1.1/32 from Device1 and Device2, and prefers to use the lines between it and Device1 to forward packets.
- Enable OSPF FRR on Device1 and Device3. When the lines between Device1 and Device3 fail, the service can quickly switch to Device2 for communication.

#### Network Topology

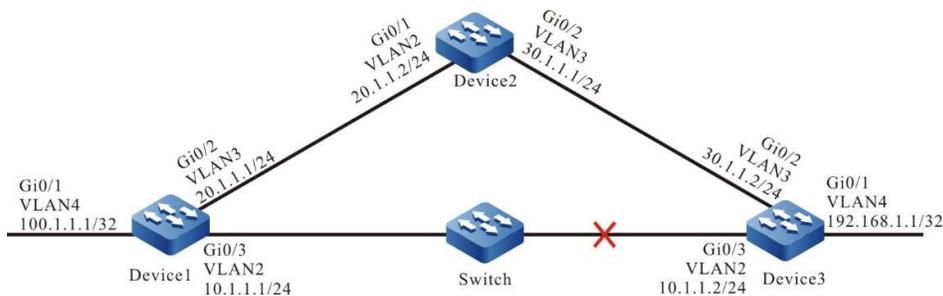


Figure 55-11 Network Topology for Configuring OSPF FRR

## Configuration Steps

Step 1: Configure VLAN, and add ports to the required VLAN; configure the IP address of each interface (Omitted).

Step 2: Configure OSPF.

#On Device1, configure OSPF process and make area 0 cover the interface.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#router-id 1.1.1.1
Device1(config-ospf)#network 10.1.1.0 0.0.0.255 area 0
Device1(config-ospf)#network 20.1.1.0 0.0.0.255 area 0
Device1(config-ospf)#network 100.1.1.1 0.0.0.0 area 0
Device1(config-ospf)#exit
```

#On Device2, configure OSPF process and make area 0 cover the interface.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#router-id 2.2.2.2
Device2(config-ospf)#network 20.1.1.0 0.0.0.255 area 0
Device2(config-ospf)#network 30.1.1.0 0.0.0.255 area 0
Device2(config-ospf)#exit
```

#On Device3, configure OSPF process and make area 0 cover the interface.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#router-id 3.3.3.3
Device3(config-ospf)#network 10.1.1.0 0.0.0.255 area 0
Device3(config-ospf)#network 30.1.1.0 0.0.0.255 area 0
Device3(config-ospf)#network 192.168.1.1 0.0.0.0 area 0
Device3(config-ospf)#exit
```

Step 3: Configure routing policy.

#On Device1, configure route-map to invoke ACL to match 192.168.1.1/32 only, and filter other networks.

The route matching the match rule applies the backup next hop interface vlan3. The next hop address is 20.1.1.2.

```
Device1(config)#ip access-list standard 1
Device1(config-std-nacl)#permit 192.168.1.1 0.0.0.0
Device1(config-std-nacl)#exit
Device1(config)#route-map ipfir_ospf
Device1(config-route-map)#match ip address 1
Device1(config-route-map)#set fast-reroute backup-interface vlan3 backup-nexthop 20.1.1.2
Device1(config-route-map)#exit
```

#On Device3, configure route-map to invoke ACL to match 100.1.1.1/32 only, and filter other networks.

The route matching the match rule applies the backup next hop interface vlan3. The next hop address is 30.1.1.1.

```
Device3(config)#ip access-list standard 1
Device3(config-std-nacl)#permit 100.1.1.1 0.0.0.0
Device3(config-std-nacl)#exit
Device3(config)#route-map ipfir_ospf
Device3(config-route-map)#match ip address 1
Device3(config-route-map)#set fast-reroute backup-interface vlan3 backup-nexthop 30.1.1.1
```

```
Device3(config-route-map)#exit
```

#### Step 4: Configure FRR.

#On Device1, enable OSPF FRR.

```
Device1(config)#router ospf 100
Device1(config-ospf)#fast-reroute route-map ipfrr_ospf
Device1(config-ospf)#exit
```

#On Device3, enable OSPF FRR.

```
Device3(config)#router ospf 100
Device3(config-ospf)#fast-reroute route-map ipfrr_ospf
Device3(config-ospf)#exit
```

#### Step 5: Check the result.

#View the routing table of Device1.

```
Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 10.1.1.0/24 is directly connected, 00:22:44, vlan2
L 10.1.1.1/32 is directly connected, 00:22:44, vlan2
C 20.1.1.0/24 is directly connected, 06:39:56, vlan3
L 20.1.1.1/32 is directly connected, 06:39:56, vlan3
O 30.1.1.0/24 [110/2] via 20.1.1.2, 00:01:51, vlan3
   [110/2] via 10.1.1.2, 00:00:16, vlan2
C 127.0.0.0/8 is directly connected, 31:14:38, lo0
L 127.0.0.1/32 is directly connected, 31:14:38, lo0
LC 100.1.1.1/32 is directly connected, 03:14:47, vlan4
O 192.168.1.1/32 [110/2] via 10.1.1.2, 00:00:04, vlan2
```

#The FRR table of Device1 shows the route of network 192.168.1.1/32. The next hop interface is vlan3.

```
Device1#show ip frr route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

O 192.168.1.1/32 [110/0] via 20.1.1.2, 00:00:08, vlan3
```

#According to the backup next hop information of Device1, the backup interface of FRR is vlan3.

```
Device1#show nexthop frr detail
Index          : 225
Type           : FRR
Reference Count : 1
Active Path    : master
Nexthop Address : 10.1.1.2
Interface      : vlan2
Interface Vrf  : global
Channel ID     : 10
Link Header Length : 18
Link Header    : 00017a123453201201010101810000010800
Action        : FORWARDING
Slot          : 0
BK Nexthop Address : 20.1.1.2
BK Interface     : vlan3
BK Interface Vrf  : global
BK Channel ID    : 11
BK Link Header Length : 18
BK Link Header   : 00017a455449201201010102810000020800
BK Action       : FORWARDING
```

BK Slot : 0

Total 1 entries.

#When the lines between Device1 and Device3 fail, it will quickly identify the failures and switch to Device2 for communication. It can be seen from the routing table and FRR table of Device1 that the output interface of the destination network 192.168.1.1/32 in the routing table has switched to the backup interface vlan3.

```
Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 10.1.1.0/24 is directly connected, 00:22:44, vlan2
L 10.1.1.1/32 is directly connected, 00:22:44, vlan2
C 20.1.1.0/24 is directly connected, 06:39:56, vlan3
L 20.1.1.1/32 is directly connected, 06:39:56, vlan3
O 30.1.1.0/24 [110/2] via 20.1.1.2, 00:01:51, vlan3
   [110/2] via 10.1.1.2, 00:00:16, vlan2
C 127.0.0.0/8 is directly connected, 31:14:38, lo0
L 127.0.0.1/32 is directly connected, 31:14:38, lo0
LC 100.1.1.1/32 is directly connected, 03:14:47, vlan4
O 192.168.1.1/32 [110/3] via 20.1.1.2, 00:00:04, vlan3
```

On Device3, it is processed in a manner which is similar to that on Device1.

# 56 OSPFv3

## 56.1 Overview

OSPFv3 is the shortened form of OSPF (Open Shortest Path First) version 3. Supporting IPv6, it follows RFC2328 and RFC2740, and allows the OSPF extension defined by other relevant RFC.

The principle of OSPFv3 is almost the same as that of OSPFv2. It simply modifies some different IP protocols and address families. Their differences are shown below:

- OSPFv3 runs based on link, while OSPFv2 runs based on network segment;
- Each link of OSPFv3 supports multiple instances;
- OSPFv3 identifies neighbors with Router ID, while OSPFv2 identifies neighbors with IP address;

## 56.2 OSPFv3 function configuration

Table 56 OSPFv3 Function Configuration List

Configuration Task	
Configure Basic Functions of OSPFv3	Enable OSPFv3 Protocol
Configure OSPFv3 Area	Configure OSPFv3 NSSA Area
	Configure OSPFv3 Stub Area
	Configure OSPFv3 Virtual Link
Configure Network Type of OSPFv3	Configure Network Type of OSPFv3 Interface as Broadcast
	Configure Network Type of OSPFv3 Interface as P2P
	Configure Network Type of OSPFv3 Interface as NBMA

Configuration Task	
	Configure Network Type of OSPFv3 Interface as P2MP
Configure OSPFv3 Network Authentication	Configure OSPFv3 Area Authentication
	Configure OSPFv3 Interface Authentication
Configure OSPFv3 Route Generation	Configure OSPFv3 Route Redistribution
	Configure OSPFv3 Default Route
Configure OSPFv3 Route Control	Configure OSPFv3 Inter-area Route Summarization
	Configure OSPFv3 External Route Summarization
	Configure OSPFv3 Inter-area Route Filtration
	Configure OSPFv3 External Route Filtration
	Configure OSPFv3 Route Installation Filtration
	Configure OSPFv3 Interface Cost Value
	Configure OSPFv3 Reference Bandwidth
	Configure OSPFv3 Administrative Distance
Configure OSPFv3 Network Optimization	Configure the Maximum Number of OSPFv3 Load Balancing Entries
	Configure Keepalive Time of OSPFv3 Neighbors
	Configure Passive OSPFv3 Interface
	Configure OSPFv3 Demand Circuit
	Configure OSPFv3 Interface Priority
	Configure OSPFv3 Interface to Ignore MTU

Configuration Task	
	Configure LSA Transfer Delay of OSPFv3 Interface
	Configure OSPFv3 LSA retransmission
	Configure OSPFv3 SPF Calculation Time
Configure OSPFv3 GR	Configure OSPFv3 GR Restarter
	Configure OSPFv3 GR Helper
Configure Coordination of OSPFv3 with BFD	Configure Coordination of OSPFv3 with BFD

### 56.2.1 Configure Basic Functions of OSPFv3

In the various configuration tasks of OSPFv3, you must first enable the OSPFv3 protocol so that the configuration of the other function features can take effect.

#### Configuration Condition

Before configuring the basic OSPFv3 functions, do the following:

- The link layer protocol has been configured to ensure normal communication at the link layer.
- Enable the IPv6 forwarding function.

#### Enable OSPFv3 Protocol

To enable the OSPFv3 function, first create an OSPFv3 process, specify the router ID of this process, and enable the OSPFv3 protocol on the interface.

The device where OSPFv3 protocol is running must have a Router ID, which is used to uniquely identify a device in an OSPFv3 AS. The uniqueness of the Router ID in the AS must be guaranteed. Otherwise, it will influence the neighbor establishment and route learning. In OSPFv3, an IPv4 address format and Router ID are required to be manually configured.

OSPFv3 supports multiple processes that are identified with process number, and different processes are independent of each other.

Table 1 Enabling OSPFv3 Protocol

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Create OSPFv3 process and enter OSPF configuration mode	<b>ipv6 router ospf</b> <i>process-id</i> [ <i>vrf vrf-name</i> ]	Mandatory Enable the OSPFv3 process directly or from VRF. By default, the OSPFv3 protocol is disabled in the system. When OSPFv3 is enabled from VRF, the OSPFv3 process belonging to a certain VRF can manage the interfaces belonging to this VRF only.
Configure the Router ID of OSPFv3 process	<b>router-id</b> <i>ipv4-address</i>	Mandatory
Return to the global configuration mode	<b>exit</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Enable the OSPFv3 protocol on the interface	<b>ipv6 router ospf</b> <i>process-id</i> <b>area</b> <i>area-id</i> [ <b>instance-id</b> <i>instance-id</i> ]	Mandatory By default, the OSPFv3 protocol is disabled on the interface.

### 56.2.2 Configure OSPFv3 Area

In order to reduce the CPU and memory usage by a large amount of database information, the OSPFv3 AS is divided into multiple areas. The area is identified by a 32-bit area ID, which can be represented by a decimal number ranging from 0 to 4294967295 or an IP address within 0.0.0.0 - 255.255.255.255. Area 0 or 0.0.0.0 means the backbone area of OSPFv3, and others are non-backbone areas. All the inter-area routing information needs to be forwarded through backbone areas. Routing information cannot be directly exchanged between non-backbone areas.

OSPFv3 defines several types of routers:

- Internal Router: The device whose all interfaces belong to the same area;

- Area Border Router (ABR): The device connecting to multiple areas;
- Autonomous System Boundary Router (ASBR): The device which imports external route for OSPFv3 AS.

### Configuration Condition

Before configuring OSPFv3 area, ensure that:

- Enable the IPv6 forwarding function.
- Enable the OSPFv3 protocol.

### Configure OSPFv3 NSSA Area

Type-7 LSA instead of Type-5 LSA is allowed to be injected into the Not-So-Stub-Area (NSSA). By configuring redistribution to import external routes to the NSSA area. The ASBR in the NSSA area generates Type-7 LSA and floods it to the NSSA area. The ABR in the NSSA area will convert Type-7 LSAs into Type-5 LSAs, and then flood these Type-5 LSAs to the entire AS.

The OSPFv3 NSSA area configured through the command **area area-id nssa no-summary** is called a totally NSSA area. The OSPFv3 totally NSSA area prohibits inter-area routes from flooding. At this time, ABR will generate a default route and flood it into the NSSA area. Devices in the NSSA area will access the networks outside the area through this default route.

Table 2 Configuring OSPFv3 NSSA Area

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter OSPFv3 configuration mode	<b>ipv6 router ospf process-id [vrf vrf-name ]</b>	-
Configure NSSA area	<b>area area-id nssa [ no-redistribution / no-summary / default-information-originate [ metric metric-value / metric-type type-value ] ]</b>	Mandatory  By default, OSPFv3 area is not a NSSA area.

---

### Note

- Backbone areas cannot be configured as NSSA areas.
  - All devices in the same NSSA area must be configured as NSSA areas. Neighbor relations cannot be formed between the devices with inconsistent area types.
-

## Configure OSPFv3 Stub Area

The Stub area does not allow AS external routes to flood. This can reduce the size of the link status database. After an area is configured as Stub, the ABR on the border of Stub will generate a default route and flood it into the Stub area. Devices in the Stub area will access the networks outside the AS through this default route.

The OSPFv3 Stub area configured through the command **area area-id stub no-summary** is called a totally Stub area. The OSPFv3 totally Stub area prohibits inter-area routes or external routes from flooding. Devices in the area will access the networks outside the area and the OSPFv3 AS through the default route.

Table 56 Configuring OSPFv3 Stub Area

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter OSPFv3 configuration mode	<b>ipv6 router ospf process-id [vrf vrf-name ]</b>	-
Configure Stub area	<b>area area-id stub [ no-summary ]</b>	Mandatory By default, OSPFv3 area is not a Stub area.

---

### Note

- Backbone areas cannot be configured as Stub areas.
  - All devices in the same Stub area must be configured as Stub areas. Neighbor relations cannot be formed between the devices with inconsistent area types.
- 

## Configure OSPFv3 Virtual Link

In OSPFv3, non-backbone areas must complete database synchronization and data interaction through backbone areas. Therefore, all non-backbone areas must connect with backbone areas.

When this requirement cannot be satisfied in some circumstances, you may configure a virtual link. After a virtual link is configured, you can configure authentication method and modify Hello time interval for the virtual link. Meanings of these parameters are consistent with those of general OSPFv3 interface parameters.

Table 3 Configuring OSPFv3 Virtual Link

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter OSPFv3 configuration mode	<b>ipv6 router ospf <i>process-id</i> [vrf <i>vrf-name</i> ]</b>	-
Configure virtual link	<b>area <i>transit-area-id</i> virtual-link <i>neighbor-id</i> [ <b>dead-interval <i>seconds</i> / hello-interval <i>seconds</i> / retransmit-interval <i>seconds</i> / transmit-delay <i>seconds</i> ]</b></b>	Mandatory  By default, no virtual link is created.

---

### Note

- Virtual link must be configured between two ABRs.
  - The two ABRs configured with virtual links must be within the same common area, which is called the Transit Area of the virtual link.
  - This Transit Area shall not be a Stub or NSSA area.
- 

## 56.2.3 Configure Network Type of OSPFv3

Depending on the link protocol type, OSPFv3 divides networks into four types:

- Broadcast Networks - When the link protocol is Ethernet or FDDI, the OSPFv3 network type is broadcast by default.
- P2P (Point To Point Network) - When the link protocol is PPP, LAPB or HDLC, the OSPFv3 network type is P2P by default.
- NBMA (Non-Broadcast Multi-Access Network) - When the link protocol is ATM, frame relay or X.25, the OSPFv3 network type is NBMA by default.
- P2MP (Point To Multi-Point Network) - No link protocol will be deemed as P2MP by OSPFv3 by default. Generally, the NBMA network which is not fully connected is configured as an OSPFv3 P2MP.

The network type of OSPFv3 interface can be modified as needed. The network types of the interfaces that establish OSPFv3 neighbors must be consistent, or the normal learning of routes will be affected.

### Configuration Condition

Before configuring OSPFv3 network type, ensure that:

- Enable the IPv6 forwarding function.
- Enable the OSPFv3 protocol.

### Configure Network Type of OSPFv3 Interface as Broadcast

Broadcast network supports multiple (more than two) devices that can exchange information with all the devices on the network. OSPFv3 uses Hello packets to dynamically find neighbors.

Table 56 Configuring Network Type of OSPFv3 Interface as Broadcast

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure Network Type of OSPFv3 Interface as Broadcast	<b>ipv6 ospf network broadcast</b>	Mandatory By default, the network type of OSPFv3 interface depends on the protocol in link layer.

### Configure Network Type of OSPFv3 Interface as P2P

Point-to-point network is the network composed of two devices, each of which is located at an end of the point-to-point link. OSPFv3 uses Hello packets to dynamically find neighbors.

Table 56 Configuring Network Type of OSPFv3 Interface as P2P

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure Network Type of OSPFv3 Interface as P2P	<b>ipv6 ospf network point-to-point</b>	Mandatory By default, the network type of OSPFv3 interface depends on the protocol in link layer.

### Configure Network Type of OSPFv3 Interface as NBMA

NBMA network supports multiple (more than two) devices. Yet it cannot broadcast, and neighbors need to be manually specified.

Table 4 Configuring Network Type of OSPFv3 Interface as NBMA

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure Network Type of OSPFv3 Interface as NBMA	<b>ipv6 ospf network non-broadcast</b>	Mandatory  By default, the network type of OSPFv3 interface depends on the protocol in link layer.
Configure NBMA network neighbors	<b>ipv6 ospf neighbor</b> <i>neighbor-ipv6-address</i> [ <b>priority</b> <i>priority-value</i> / <b>poll-interval</b> <i>interval-value</i> / <b>cost</b> <i>cost-value</i> ] [ <b>instance-id</b> <i>instance-id</i> ]	Mandatory  In NBMA network, neighbors need to be manually specified.

#### Configure Network Type of OSPFv3 Interface as P2MP

When NBMA is not fully connected, the network type can be configured as P2MP to save network cost. When the network type is configured as P2MP unicast, neighbors need to be manually specified.

Table 5 Configuring Network Type of OSPFv3 Interface as P2MP

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure Network Type of OSPFv3 Interface as P2MP	<b>ipv6 ospf network point-to-multipoint</b> [ <b>non-broadcast</b> ]	Mandatory  By default, the network type of OSPFv3 interface depends on the protocol in link layer.

Step	Command	Description
Configure P2MP unicast network neighbors	<b>ipv6 ospf neighbor</b> <i>neighbor-ipv6-address</i> [ <b>priority</b> <i>priority-value</i> / <b>poll-interval</b> <i>interval-value</i> / <b>cost</b> <i>cost-value</i> ] [ <b>instance-id</b> <i>instance-id</i> ]	If the network type of interface is configured as P2MP, it is mandatory

#### 56.2.4 Configure OSPFv3 Network Authentication

In order to avoid information leakage or malicious attacks on OSPFv3 devices, all packet interactions between OSPFv3 neighbors can realize encryption and authentication. The encryption & authentication type and algorithm can be NULL (no authentication), SHA1 authentication, and MD5 authentication specified by the IPsec encryption & authentication policy.

After authentication is configured, the IPsec security feature can encrypt and authenticate OSPFv3 protocol packets. The OSPFv3 protocol can receive packets only when they pass decryption and authentication. Therefore, for the OSPFv3 interfaces that establish neighbor relations, their authentication method, Spi ID, and the IPsec encryption & authentication policy configured for authentication password must be consistent. The OSPFv3 authentication method can be configured on areas and interfaces. In particular, area authentication has a lower priority than interface authentication. That is to say, you are required to first use interface authentication and then area authentication.

##### Configuration Condition

Before configuring OSPFv3 network authentication, ensure that:

- Enable the IPv6 forwarding function.
- Enable the OSPFv3 protocol.

##### Configure OSPFv3 Area Authentication

Configuring area authentication in the OSPFv3 process area can make all interfaces in the area use area authentication. This can effectively avoid repeated configuration of the same network authentication method for the interface.

Table 6 Configuring OSPFv3 Area Authentication

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter OSPFv3 configuration mode	<b>ipv6 router ospf</b> <i>process-id</i> [ <b>vrf</b> <i>vrf-name</i> ]	-

Configure area authentication	<b>area <i>area-id</i> ipsec-tunnel <i>tunnel-name</i></b>	Mandatory  By default, no OSPFv3 area authentication is configured.
-------------------------------	--	---

### Configure OSPFv3 Interface Authentication

When an interface has multiple OSPFv3 instances, you can specify authentication method and password for an instance separately. The authentication method specified under the area is applicable to the instances where interface authentication is not specified under the interface.

Table 7 Configuring OSPFv3 Interface Authentication

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface <i>interface-name</i></b>	-
Configure interface authentication method	<b>ipv6 ospf ipsec-tunnel <i>tunnel-name</i>{<i>instance-id</i> <i>instance-id</i>}</b>	Mandatory  By default, no OSPFv3 interface authentication is configured.

## 56.2.5 Configure OSPFv3 Route Generation

### Configuration Condition

Before configuring OSPFv3 route generation, ensure that:

- Enable the IPv6 forwarding function.
- Enable the OSPFv3 protocol.

### Configure OSPFv3 Route Redistribution

When multiple routing protocols are running on a device, routes of other protocols are imported into OSPFv3 through redistribution to generate OSPFv3 external type-2 routes by default, with the routing metric value being 20. When external routes are imported through redistribution, you can modify the type of external route, metric, and Tag fields, and associate the specified routing policy for route control and management.

Table 8 Configuring OSPFv3 Route Redistribution

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter OSPFv3 configuration mode	<b>ipv6 router ospf</b> <i>process-id</i> [ <b>vrf</b> <i>vrf-name</i> ]	-
Configure OSPFv3 Route Redistribution	<b>redistribute</b> <i>routing-protocol</i> [ <i>protocol-id-or-name</i> ] [ <b>metric</b> <i>metric-value</i> / <b>metric-type</b> <i>type-value</i> / <b>tag</b> <i>tag-value</i> / <b>route-map</b> <i>map-name</i> / <b>match</b> <i>route-type</i> ]	Mandatory By default, no OSPFv3 route redistribution is configured.
Configure the metric value of OSPFv3 external route	<b>default-metric</b> <i>metric-value</i>	Optional

## Note

- When redistribute protocol [protocol-id] metric and default-metric are both configured to set the metric value of external route, the former has a higher priority.

### Configure OSPFv3 Default Route

After the OSPFv3 Stub area and totally NSSA area are configured, a Type-3 default route will be automatically generated. Default route cannot be automatically generated in NSSA area. But a Type-7 default route can be imported to this area through the command **area** *area-id* **nssa default-information-originate**.

OSPFv3 cannot import Type-5 default route through the **redistribute** command. When necessary, the **default-information originate [always]** command can be used to achieve this purpose.

Table 9 Configuring OSPFv3 Default Route

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter OSPFv3 configuration mode	<b>ipv6 router ospf</b> <i>process-id</i> [ <b>vrf</b> <i>vrf-name</i> ]	-

Step	Command	Description
Configure OSPFv3 Default Route	<b>default-information originate</b> [ <b>always</b> / <b>metric</b> <i>metric-value</i> / <b>metric-type</b> <i>metric-type</i> / <b>route-map</b> <i>route-map-name</i> ]	<p>Mandatory</p> <p>By default, no external default route will be imported into OSPFv3 AS.</p> <p>For the default route imported, the default metric value is 1, and the type is external type-2.</p> <p><b>always</b> means that the default route is required to be generated in OSPFv3 AS. Otherwise, it will be generated only when there is a default route in the local routing table.</p>

## 56.2.6 Configure OSPFv3 Route Control

### Configuration Condition

Before configuring OSPFv3 route control, ensure that:

- Enable the IPv6 forwarding function.
- Enable the OSPFv3 protocol.

### Configure OSPFv3 Inter-area Route Summarization

When the ABR in OSPFv3 advertises inter-area routes to other areas, each route is advertised separately as Type-3 LSAs. You may use the inter-area route summarization function to summarize some contiguous network segments in the area into one route to advertise the summarized route only. This can reduce the size of the OSPFv3 database.

Table 10 Configuring OSPFv3 Inter-area Route Summarization

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter OSPFv3 configuration mode	<b>ipv6 router ospf</b> <i>process-id</i> [ <b>vrf</b> <i>vrf-name</i> ]	-

Step	Command	Description
Configure OSPFv3 Inter-area Route Summarization	<b>area area-id range ipv6-prefix/prefix-length [ advertise   not-advertise]</b>	Mandatory By default, ABR doesn't conduct inter-area route summarization.

---

### Note

- The OSPFv3 inter-area route summarization function takes effect on ABR only.
  - By default, the minimum cost value of detail routes is selected as the cost value of summarized route.
- 

### Configure OSPFv3 External Route Summarization

When OSPFv3 redistributes external routes, each route is advertised separately in external link status advertisement. You may use the external route summarization function to summarize some contiguous network segments outside the AS into one route to advertise the summarized route only. This can reduce the size of the OSPFv3 database.

After configuring the command **summary-address** on ASBR, you can summarize the Type-5 LSA and Type-7 LSA within the scope of summarized address.

Table 11 Configuring OSPFv3 External Route Summarization

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter OSPFv3 configuration mode	<b>ipv6 router ospf process-id [vrf vrf-name]</b>	-
Configure OSPFv3 External Route Summarization	<b>summary-prefix ipv6-prefix/prefix-length [ not-advertise   tag tag-value]</b>	Mandatory By default, ABR doesn't conduct external route summarization.

---

### Note

- The OSPFv3 external route summarization function takes effect on ASBR only.

### Configure OSPFv3 Inter-area Route Filtration

When ABR is receiving inter-area route, ACL or prefix list is used for filtration in the incoming function; when it is advertising inter-area route, ACL or prefix list is used for filtration in the outgoing function.

Table 12 Configuring OSPFv3 Inter-area Route Filtration

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter OSPFv3 configuration mode	<b>ipv6 router ospf process-id [vrf vrf-name ]</b>	-
Configure OSPFv3 Inter-area Route Filtration	<b>area area-id filter-list { access { access-list-name / access-list-number }   prefix prefix-list-name } { in   out }</b>	Mandatory By default, ABR doesn't conduct inter-area route filtration.

### Note

- The OSPFv3 inter-area route filtration function takes effect on ABR only.

### Configure OSPFv3 External Route Filtration

Configure external route filtration, i.e. apply ACL or prefix list to allow or prohibit the flooding of routes into OSPFv3 AS from outside.

Table 13 Configuring OSPFv3 External Route Filtration

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter OSPFv3 configuration mode	<b>ipv6 router ospf process-id [vrf vrf-name ]</b>	-
Configure OSPFv3 External Route Filtration	<b>distribute-list { access { access-list-name / access-list-number }   prefix prefix-</b>	Mandatory

Step	Command	Description
	<i>list-name</i> } <b>out</b> [ <i>routing-protocol</i> [ <i>process-id</i> ] ]	By default, ASBR doesn't conduct external route filtration.

---

## Note

- The OSPFv3 external route filtration function takes effect on ASBR only.
- 

### Configure OSPFv3 Route Installation Filtration

After OSPFv3 calculates routes through LSA, the calculated OSPFv3 protocol routing information can be filtered to prevent certain routes from being added to the routing table.

Table 14 Configuring OSPFv3 Route Installation Filtration

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter OSPFv3 configuration mode	<b>ipv6 router ospf</b> <i>process-id</i> [ <i>vrf vrf-name</i> ]	-
Configure OSPFv3 Route Installation Filtration	<b>distribute-list</b> { <b>access</b> { <i>access-list-name</i>   <i>access-list-number</i> }   <b>gateway</b> <i>prefix-list-name1</i>   <b>prefix</b> <i>prefix-list-name2</i> [ <b>gateway</b> <i>prefix-list-name3</i> ]   <b>route-map</b> <i>route-map-name</i> } <b>in</b> [ <i>interface-name</i> ]	Mandatory By default, no OSPFv3 route installation filtration is configured.

---

## Note

- Make prefix, gateway and route-map filtration and ACL filtration mutually exclusive. For example, if prefix filtration has been configured, ACL filtration cannot be configured.
  - Make route-map and prefix filtration and gateway filtration mutually exclusive.
  - Make prefix filtration and gateway filtration cover each other.
-

### Configure OSPFv3 Interface Cost Value

By default, the OSPFv3 interface cost is calculated with the following methods: reference bandwidth/interface bandwidth.

Table 15 Configuring OSPFv3 Interface Cost Value

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure OSPFv3 Interface Cost Value	<b>ipv6 ospf cost</b> <i>cost</i> [ <b>instance-id</b> <i>instance-id</i> ]	Optional By default, the calculation is conducted according to the reference bandwidth/interface bandwidth.

### Configure OSPFv3 Reference Bandwidth

The reference bandwidth of interface is mainly used to calculate interface cost value which is 100Mbit/s by default. The OSPFv3 interface cost is calculated with the following methods: reference bandwidth/interface bandwidth. When the calculation result is greater than 1, take the integer part; when it is less than 1, take 1. Therefore, in a network with a bandwidth higher than 100Mbit/s, the optimal route cannot be correctly selected. To solve this problem, the **auto-cost reference-bandwidth** command can be used to configure appropriate reference bandwidth.

Table 16 Configuring OSPFv3 Reference Bandwidth

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter OSPFv3 configuration mode	<b>ipv6 router ospf</b> <i>process-id</i> [ <b>vrf</b> <i>vrf-name</i> ]	-
Configure OSPFv3 Reference Bandwidth	<b>auto-cost reference-bandwidth</b> <i>reference-bandwidth</i>	Optional By default, the reference bandwidth is 100Mbit/s.

### Configure OSPFv3 Administrative Distance

Administrative distance indicates the reliability of routing protocol. When the routes that reach the same destination network are learned from different routing protocols, they are selected according to the administrative distance. Those with a small administrative distance are selected first.

Table 17 Configuring OSPFv3 Administrative Distance

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter OSPFv3 configuration mode	<b>ipv6 router ospf</b> <i>process-id</i> [ <b>vrf</b> <i>vrf-name</i> ]	-
Configure OSPFv3 Administrative Distance	<b>distance [ ospf { external distance / inter-area distance / intra-area distance }   distance ]</b>	Optional By default, the administrative distance of intra-area and inter-area routes of OSPFv3 is 110, and that of external routes is 150.

#### Configure the Maximum Number of OSPFv3 Load Balancing Entries

If there are multiple equal-cost paths leading to the same destination address, the paths form load balancing, which can improve the link utility rate and reduce the load of links.

Table 18 Configuring Maximum Number of Load Balancing Entries of OSPFv3

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter OSPFv3 configuration mode	<b>ipv6 router ospf</b> <i>process-id</i> [ <b>vrf</b> <i>vrf-name</i> ]	-
Configure the Maximum Number of OSPFv3 Load Balancing Entries	<b>maximum-paths</b> <i>max-number</i>	Optional By default, the maximum number of load balancing entries of OSPFv3 is 4.

## 56.2.7 Configure OSPFv3 Network Optimization

### Configuration Condition

Before configuring OSPFv3 network optimization, ensure that:

- Enable the IPv6 forwarding function.
- Enable the OSPFv3 protocol.

### Configure Keepalive Time of OSPFv3 Neighbors

OSPFv3 Hello packets are used to establish and keep alive neighbor relationships. The default time interval of sending Hello packets depends on the network type. In broadcast and P2P networks, it is 10 seconds, and in P2MP and NBMA networks, it is 30 seconds.

The failure time of neighbor is used to identify the validity of the neighbor. By default, it is 4 times the Hello time interval. If the OSPFv3 device does not receive the Hello packets from the neighbor after time out of its failure time, the neighbor is considered invalid and deleted.

Table 19 Configuring Keepalive Time of OSPFv3 Neighbor

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure OSPFv3 Hello time interval	<b>ipv6 ospf hello-interval</b> <i>interval-value</i> [ <b>instance-id</b> <i>instance-id</i> ]	Optional The default value is determined based on network class. For broadcast and P2P networks, it's 10 seconds; for P2MP and NBMA networks, it's 30 seconds.
Configure failure time interval of OSPFv3 neighbors	<b>ipv6 ospf dead-interval</b> <i>interval-value</i> [ <b>instance-id</b> <i>instance-id</i> ]	Optional The default value is 4 times the Hello interval.



- The Hello interval between adjacent OSPFv3 devices must be the same as the failure time of neighbor. Otherwise, the neighbor relationship cannot be established.
- When modifying Hello interval, if the failure time of current neighbor is 4 times the Hello interval, the failure time of neighbor will also be automatically modified so that it is 4 times the Hello interval; if the failure time of current neighbor is not 4 times the Hello interval, the failure time of neighbor will remain unchanged.
- Modifying the failure time of neighbor will not affect the Hello interval.

### Configure Passive OSPFv3 Interface

Dynamic routing protocol uses passive interface, which can effectively reduce the consumption of network bandwidth by routing protocol. Configure passive OSPFv3 interface to enable the command to advertise the route of the direct network segment where the interface is located. But it will suppress the receiving and sending of OSPFv3 protocol packets on this interface.

Table 20 Configuring Passive OSPFv3 Interface

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter OSPFv3 configuration mode	<b>ipv6 router ospf</b> <i>process-id</i> <b>[vrf</b> <i>vrf-name</i> <b>]</b>	-
Configure Passive OSPFv3 Interface	<b>passive-interface</b> <i>{interface-name   default}</i>	Mandatory By default, no passive OSPF interface is configured.

### Configure OSPFv3 Demand Circuit

On P2P and P2MP links, to reduce line costs, you can configure OSPFv3 demand circuit to suppress the periodic sending of Hello packets and periodic refresh of LSA packets. It is mainly applied in paid links, such as ISDN, SVC and X.25.

Table 21 Configuring OSPFv3 Demand Circuit

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-

Step	Command	Description
Configure OSPFv3 Demand Circuit	<b>ipv6 ospf demand-circuit</b> [ <b>instance-id</b> <i>instance-id</i> ]	Mandatory  By default, the OSPFv3 demand circuit is disabled.

### Configure OSPFv3 Interface Priority

Interface priority is mainly applied in the election of DR (Designed Router) and BDR (Backup Designed Router) in broadcast and NBMA networks. The value ranges from 0 to 255. The larger the value, the higher the priority. The default value is 1.

DR and BDR are elected by all the devices in the same network segment according to interface priority and Router ID through Hello packets. The rules are shown below:

- Firstly, the device with the highest interface priority is elected as the DR, and that with the second interface priority as the BDR. The device with the priority of 0 does not participate in the election.
- If the interface priorities are the same, the device with the highest router ID is elected as the DR, and that with the second router ID as the BDR.

After the DR fails, BRD will become a DR immediately, and a new BDR will be elected.

Table 22 Configuring OSPFv3 Interface Priority

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure OSPFv3 Interface Priority	<b>ipv6 ospf priority</b> <i>priority-value</i> [ <b>instance-id</b> <i>instance-id</i> ]	Optional  By default, the OSPFv3 interface priority is 1.

### Note

- Priority affects the election process only. When DR and BDR have been elected in the network, modifying interface priority will affect the next election result only. Therefore, DR is not necessarily the device with the highest interface priority, and DBR is not necessarily the device with the second high interface priority.

### Configure OSPFv3 Interface to Ignore MTU

When adjacent OSPFv3 devices exchange DD packets with each other, they will check whether the MTUs are the same by default. If different, a neighbor relation cannot be established. After OSPFv3 is configured to ignore interface MTU check, even if the MTUs are different, the neighbor relation can be established.

Table 23 Configuring OSPFv3 Interface to Ignore MTU

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure OSPFv3 Interface to Ignore MTU	<b>ipv6 ospf mtu-ignore</b> [ <b>instance-id</b> <i>instance-id</i> ]	Mandatory By default, MTU check will be conducted. consistency check

### Configure LSA Transfer Delay of OSPFv3 Interface

LSA transfer delay means the period during which LSA floods to other devices. The device sending LSA will add the interface transfer delay time to the aging time of the LSA to be sent. By default, when the flooded LSA passes through a device, the aging time increases by 1. The transfer delay of LSA can be configured according to network conditions, from 1 to 840. It is generally used on low-speed links.

Table 24 Configuring OSPFv3 Interface LSA Transfer Delay

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure LSA Transfer Delay of OSPFv3 Interface	<b>ipv6 ospf transmit-delay</b> <i>delay-value</i> <b>instance-id</b> [ <i>instance-id</i> ]	Optional By default, the LSA transfer delay is 1 second.

### Configure OSPFv3 LSA retransmission

In order to ensure the reliability of data interaction, OSPFv3 uses the acknowledgement mechanism. When an LSA is flooded on the device interface, it will be added to the neighbor's retransmission list. If

confirmation is not received from the neighbor after the retransmission time expires, this LSA will be retransmitted until the confirmation is received.

Table 25 Configuring OSPFv3 LSA Retransmission

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure OSPFv3 LSA retransmission interval	<b>ipv6 ospf retransmit-interval</b> <i>interval-value</i> [ <b>instance-id</b> <i>instance-id</i> ]	Optional By default, the LSA retransmission interval is 5 seconds.

#### Configure OSPFv3 SPF Calculation Time

When the OSPFv3 network topology changes, recalculation of routes is required. When the network keeps changing, frequent routing calculation will occupy a large amount of system resources. The consumption of system resources by frequent network changes can be suppressed by adjusting the time parameters of SPF calculation.

Table 26 Configuring OSPFv3 SPF Calculation Time

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter OSPFv3 configuration mode	<b>ipv6 router ospf</b> <i>process-id</i> [ <b>vrf</b> <i>vrf-name</i> ]	-
Configure OSPFv3 SPF Calculation Time	<b>timers throttle spf</b> <i>delay-time</i> <i>hold-time</i> <i>max-time</i>	Optional By default, the <i>delay-time</i> , <i>hold-time</i> and <i>max-time</i> are 5000 milliseconds, 10000 milliseconds, and 10000 milliseconds, respectively.



**Note**

- Delay-time means the initial calculation delay, hold-time the suppression time, and max-time the maximum waiting time for two SPF calculations. When there are infrequent network changes, the continuous route calculation interval is decreased to delay-time. In the case of frequent network changes, adjustment should be made accordingly by increasing the hold-time $\times 2^{n-2}$  (n is the times of continuously triggering route calculation) to prolong the waiting time by the increment of the hold-time configured, max-time at most.

## 56.2.8 Configure OSPFv3 FRR

### Configuration Condition

Before configuring OSPFv3 FRR, ensure that:

- Enable the IPv6 forwarding function.
- Enable the OSPFv3 protocol.

### Configure OSPFv3 FRR

In the OSPFv3 network, as a result of link or device failure, the packets passing the point of failure will be discarded or loops will be produced. The traffic interruption caused thereby will continue until the protocol reconverges after several seconds. In order to reduce the time of traffic interruption, OSPFv3 FRR can be configured. By applying the routing map, set a backup next hop for the successfully matched route. Once the main link fails, the traffic passing through the failed link will immediately switch to the backup link, achieving the purpose of fast switching.

Table 27 Configuring OSPFv3 FRR

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter OSPFv3 configuration mode	<b>ipv6 router ospf process-id [vrf vrf-name ]</b>	-
Configure OSPFv3 process to enable the static FRR function	<b>fast-reroute route-map route-map-name</b>	Mandatory By default, the OSPFv3 static FRR function is disabled.
Configure OSPFv3 process to enable the dynamic FRR function	<b>fast-reroute loop-free-alternate [route-map route-map-name]</b>	Mandatory By default, the OSPFv3 dynamic FRR function is disabled.

Step	Command	Description
Configure OSPFv3 process to enable the pic function	<b>pic</b>	<p>Mandatory</p> <p>After the pic function is enabled, the auto FRR function is enabled.</p> <p>By default, the OSPFv3 function is disabled.</p>

---

### Note

- The OSPFv3 FRR function has two types, i.e. static FRR and dynamic FRR.
  - Static FRR needs to associate route-map where the next hop interface and address of back-up route are set.
  - Currently, dynamic FRR supports point-to-point network only, i.e. all the output interfaces of the device have a network type of point-to-point. After dynamic FRR is configured, the device automatically calculates and sets back-up next hop interface and address. Dynamic FRR can also associate route-map to set back-up next hop interface and address for the route which matches the route-map only.
  - The methods of enabling route redistribution are mutually exclusive.
- 

## 56.2.9 Configure OSPFv3 GR

GR (Graceful Restart) is used to keep the routing information in the forwarding layer of this device and neighbor device unchanged during the switch between host and standby devices to ensure the forwarding process is not affected; after the device is switched for re-running, the two devices synchronize routing information and update forwarding layer in the protocol layer so that the data can keep forwarding during the process of device switch.

There are two types of roles in the GR process:

- GR Restarter end: The device for graceful restart of protocol.
- GR Helper end: The device which helps with the graceful restart of protocol.

The distributed device can act as GR Restarter and GR Helper, while the centralized device only serves as GR Helper to help the Restarter complete GR.

### Configuration Condition

Before configuring OSPFv3 GR, ensure that:

- Enable the IPv6 forwarding function.

- Enable the OSPFv3 protocol.

### Configure OSPFv3 GR Restarter

Table 28 Configuring OSPFv3 GR Restarter

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter OSPFv3 configuration mode	<b>ipv6 router ospf <i>process-id</i> [ vrf <i>vrf-name</i> ]</b>	-
Configure OSPFv3 GR	<b>nsf ietf</b>	Mandatory  By default, the GR function is disabled.  After this function takes effect, the protocol needs to support the Opaque-LSA function, and it supports the Opaque-LSA function by default.
Configure OSPFv3 GR period	<b>nsf interval <i>grace-period</i></b>	Optional  By default, the GR period is 120 seconds.

#### Note

- The OSPFv3 GR function can only be used in the stacking environment or a dual-master environment.

### Configure OSPFv3 GR Helper

GR Helper can help the Restarter end complete GR. By default, the device enables this function. Users can disable this function via the command **nsf ietf helper disable**. The command **nsf ietf helper strict-lsa-checking** is used to enable the Helper end to strictly check LSA in the GR process. If any change of LSA is found, the GR Helper mode will be exited.

Table 29 Configuring OSPFv3 GR Helper

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter OSPFv3 configuration mode	<b>ipv6 router ospf process-id [ vrf vrf-name ]</b>	-
Configure OSPFv3 GR Helper	<b>nsf ietf helper [ disable   strict-lsa-checking ]</b>	Optional By default, the Helper function is enabled, but it doesn't check LSA.

## 56.2.10 Configure Coordination of OSPFv3 with BFD

### Configuration Condition

Before configuring the coordination of OSPFv3 with BFD, ensure that:

- Enable the IPv6 forwarding function.
- Enable the OSPFv3 protocol.

### Configure Coordination of OSPFv3 with BFD

BFD (Bidirectional Forwarding Detection) provides a method to quickly detect the status of lines between two devices. When BFD detection is enabled between two adjacent OSPFv3 devices, if there is a line failure between the devices, BFD can quickly detect the failure and notify the OSPFv3 protocol to trigger OSPFv3 for route calculation and switch to the backup route. In this way, it can reach the purpose of fast route switch.

Table 30 Configuring Coordination of OSPFv3 with BFD

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface interface-name</b>	-
Configure the specified OSPFv3 interface to enable or disable BFD	<b>ipv6 ospf bfd [disable] [instance-id instance-id]</b>	Mandatory By default, the BFD function is not enabled.

Step	Command	Description
Enter the global configuration mode.	<b>exit</b>	-
Enter OSPFv3 configuration mode	<b>ipv6 router ospf</b> <i>process-id</i> <b>[vrf vrf-name ]</b>	-
Configure all interfaces of OSPFv3 process to enable BFD	<b>bfd all-interfaces</b>	Optional

### Note

- When BFD is configured in OSPFv3 configuration mode and interface configuration mode at the same time, the latter has a higher priority.

## 56.2.11 OSPFv3 monitoring and maintaining

Table 31 OSPFv3 Monitoring and Maintaining

Command	Description
<b>clear ipv6 ospf err-statistic</b>	Clear error statistics of OSPFv3
<b>clear ipv6 ospf</b> [ <i>process-id</i> ] <b>process</b>	Reset OSPFv3 process
<b>clear ipv6 ospf</b> [ <i>process-id</i> ] <b>redistribution</b>	Re-advertise external route
<b>clear ipv6 ospf</b> [ <i>process-id</i> ] <b>route</b>	Recalculate OSPFv3 route
<b>clear ipv6 ospf statistics</b> [ <i>interface-name</i> ]	Clear interface statistics of OSPFv3
<b>show ipv6 ospf</b> [ <i>process-id</i> ]	Show basic information of OSPFv3
<b>show ipv6 ospf</b> [ <i>process-id</i> ] <b>border-routers</b>	Show information of the route reaching edge device in OSPFv3
<b>show ipv6 ospf core-info</b>	Show core information of OSPFv3 process
<b>show ipv6 ospf</b> [ <i>process-id</i> ] <b>database</b> [ <b>database-summary</b>   <b>external</b> / inter-prefix   <b>inter-router</b>   <b>intra-prefix</b>   <b>link</b>	Show database information of OSPFv3

Command	Description
<b>network</b>   nssa-external   grace   router   adv-router <i>router-id</i>   age <i>lsa_age</i>   max-age   self-originate]	
<b>show ipv6 ospf error-statistic</b>	Show error statistics of OSPFv3
<b>show ipv6 ospf event-list</b>	Show OSPFv3 packet receive queue information
<b>show ipv6 ospf interface</b> [ <i>interface-name</i> [ detail ] ]	Show information of OSPFv3 interface
<b>show ipv6 ospf</b> [ <i>process-id</i> ] neighbor [ <i>neighbor-id</i>   all   detail [ all ]   interface <i>interface-name</i> [ detail ]   statistics ]	Show information of OSPFv3 neighbor
<b>show ipv6 ospf</b> [ <i>process-id</i> ] route [ <i>ipv6-prefix/prefix-length</i>   connected   external   inter-area   intra-area   statistic ]	Show information of OSPFv3 route
<b>show ipv6 ospf</b> [ <i>process-id</i> ] sham-link	Show the OSPFv3 pseudo-class link interface information configured, including interface status, cost value, and neighbor status
<b>show ipv6 ospf</b> [ <i>process-id</i> ] topology area [ <i>area-id</i> ]	Show information of OSPFv3 topology
<b>show ipv6 ospf</b> [ <i>process-id</i> ] virtual-links	Show information of OSPFv3 virtual link
<b>show ipv6 ospf</b> [ vrf <i>vrf-name</i> ]	Show all OSPFv3 process information and parameters in the specified vrf
<b>show running-config ipv6 router ospf</b>	Show current running configuration of OSPFv3

## 56.3 Typical configuration example of OSPFv3

### 56.3.1 Configure Basic Functions of OSPFv3

#### Network Requirements

- All devices are configured with OSPFv3 protocol, and there are three areas, i.e. area 0, 1 and 2. Upon completion of the configuration, all the devices can learn routes from

each other.

- On the back-to-back Ethernet interface, in order to speed up the the process of establishing OSPF neighbors, the network type of OSPFv3 interface can be changed to point-to-point. Modify the network type of the interface in area 2 as point-to-point. Upon completion of the configuration, all the devices can learn routes from each other.

### Network Topology

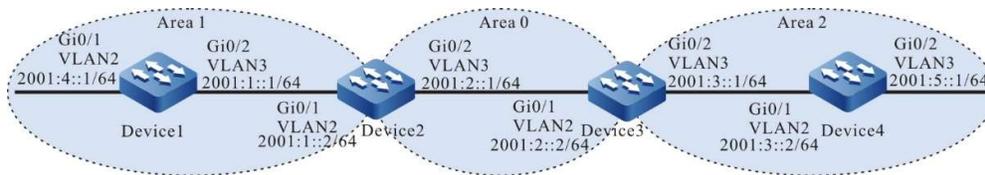


Figure 56 Network Topology for Configuring Basic Functions of OSPFv3

### Configuration Steps

- Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)
- Step 2: Configure IPv6 addresses for the ports. (Omitted)
- Step 3: Configure OSPFv3 process and make different areas cover corresponding interfaces.

#On Device1, configure OSPFv3 process and make area 1 cover the interface.

```
Device1#configure terminal
Device1(config)#ipv6 router ospf 100
Device1(config-ospf6)#router-id 1.1.1.1
Device1(config-ospf6)#exit
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ipv6 router ospf 100 area 1
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan3
Device1(config-if-vlan3)#ipv6 router ospf 100 area 1
Device1(config-if-vlan3)#exit
```

#On Device2, configure OSPFv3 process and make area 0 and 1 cover corresponding interfaces.

```
Device2#configure terminal
Device2(config)#ipv6 router ospf 100
Device2(config-ospf6)#router-id 2.2.2.2
Device2(config-ospf6)#exit
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ipv6 router ospf 100 area 1
Device2(config-if-vlan2)#exit
Device2(config)#interface vlan3
Device2(config-if-vlan3)#ipv6 router ospf 100 area 0
Device2(config-if-vlan3)#exit
```

#On Device3, configure OSPFv3 process and make area 0 and 2 cover corresponding interfaces.

```
Device3#configure terminal
Device3(config)#ipv6 router ospf 100
Device3(config-ospf6)#router-id 3.3.3.3
Device3(config-ospf6)#exit
Device3(config)#interface vlan2
Device3(config-if-vlan2)#ipv6 router ospf 100 area 0
```

```

Device3(config-if-vlan2)#exit
Device3(config)#interface vlan3
Device3(config-if-vlan3)#ipv6 router ospf 100 area 2
Device3(config-if-vlan3)#exit

```

#On Device4, configure OSPFv3 process and make area 2 cover the interface.

```

Device4#configure terminal
Device4(config)#ipv6 router ospf 100
Device4(config-ospf6)#router-id 4.4.4.4
Device4(config-ospf6)#exit
Device4(config)#interface vlan2
Device4(config-if-vlan2)#ipv6 router ospf 100 area 2
Device4(config-if-vlan2)#exit
Device4(config)#interface vlan3
Device4(config-if-vlan3)#ipv6 router ospf 100 area 2
Device4(config-if-vlan3)#exit

```

---

## Note

- In OSPFv3, Router ID must be manually configured, and the Router IDs of any routers in the AS must be different.
  - When the interface is enabled to OSPFv3, it's necessary to specify which interface instance is enabled to the OSPFv3 process, and the instance numbers on both sides must be the same, in instance 0 by default.
- 

#View OSPFv3 neighbors' information and routing table on Device1.

```

Device1#show ipv6 ospf neighbor
OSPFv3 Process (100)
Neighbor ID  Pri  State      Dead Time  Interface      Instance ID
2.2.2.2      1  Full/DR   00:00:38  vlan3          0

Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L  ::1/128 [0/0]
   via ::, 00:41:07, lo0
C  2001:1::/64 [0/0]
   via ::, 00:32:19, vlan3
L  2001:1::1/128 [0/0]
   via ::, 00:32:18, lo0
O  2001:2::/64 [110/2]
   via fe80::201:7aff:fe5e:6d45, 00:23:06, vlan3
O  2001:3::/64 [110/3]
   via fe80::201:7aff:fe5e:6d45, 00:23:00, vlan3
C  2001:4::/64 [0/0]
   via ::, 00:16:46, vlan2
L  2001:4::1/128 [0/0]
   via ::, 00:16:45, lo0
O  2001:5::/64 [110/4]
   via fe80::201:7aff:fe5e:6d45, 00:01:42, vlan3

```

#View the OSPFv3 neighbors and routing table on Device2.

```

Device2#show ipv6 ospf neighbor
OSPFv3 Process (100)
Neighbor ID  Pri  State      Dead Time  Interface      Instance ID

```

```

1.1.1.1    1 Full/Backup 00:00:34 vlan2    0
3.3.3.3    1 Full/DR     00:00:33 vlan3    0

```

```

Device2#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

```

```

L ::1/128 [0/0]
  via ::, 00:50:36, lo0
C 2001:1::/64 [0/0]
  via ::, 00:43:05, vlan2
L 2001:1::2/128 [0/0]
  via ::, 00:43:04, lo0
C 2001:2::/64 [0/0]
  via ::, 00:40:01, vlan3
L 2001:2::1/128 [0/0]
  via ::, 00:39:57, lo0
O 2001:3::/64 [110/2]
  via fe80::2212:1ff:fe01:101, 00:34:00, vlan3
O 2001:4::/64 [110/2]
  via fe80::201:7aff:fe61:7a24, 00:27:28, vlan2
O 2001:5::/64 [110/3]
  via fe80::2212:1ff:fe01:101, 00:12:41, vlan3

```

### #View the OSPFv3 LSDB (Link State Database) on Device2.

```
Device2#show ipv6 ospf database
```

```
OSPFv3 Router with ID (2.2.2.2) (Process 100)
```

```
Link-LSA (Interface vlan2)
```

Link State ID	ADV Router	Age	Seq#	CkSum	Prefix
0.0.0.1	1.1.1.1	81	0x80000001	0x8d18	1
0.0.0.1	2.2.2.2	78	0x80000001	0xf996	1

```
Link-LSA (Interface vlan3)
```

Link State ID	ADV Router	Age	Seq#	CkSum	Prefix
0.0.0.2	2.2.2.2	71	0x80000003	0x2467	1
0.0.0.1	3.3.3.3	35	0x80000003	0xcd12	1

```
Router-LSA (Area 0.0.0.0)
```

Link State ID	ADV Router	Age	Seq#	CkSum	Link
0.0.0.0	2.2.2.2	37	0x80000004	0x0dd6	1
0.0.0.0	3.3.3.3	25	0x80000007	0xda03	1

```
Network-LSA (Area 0.0.0.0)
```

Link State ID	ADV Router	Age	Seq#	CkSum
0.0.0.1	3.3.3.3	35	0x80000001	0x5790

```
Inter-Area-Prefix-LSA (Area 0.0.0.0)
```

Link State ID	ADV Router	Age	Seq#	CkSum	Prefix
0.0.0.2	2.2.2.2	42	0x80000007	0x9e25	2001:1::/64
0.0.0.3	2.2.2.2	23	0x80000002	0xcef4	2001:4::/64
0.0.0.1	3.3.3.3	35	0x80000005	0xaa16	2001:3::/64
0.0.0.3	3.3.3.3	55	0x80000001	0xc0fe	2001:5::/64

```
Intra-Area-Prefix-LSA (Area 0.0.0.0)
```

Link State ID	ADV Router	Age	Seq#	CkSum	Prefix	Reference
0.0.0.3	3.3.3.3	34	0x80000001	0xb2d3	1	Network-LSA

```
Router-LSA (Area 0.0.0.1)
```

Link State ID	ADV Router	Age	Seq#	CkSum	Link
---------------	------------	-----	------	-------	------

```
0.0.0.0 1.1.1.1 41 0x80000004 0xc726 1
0.0.0.0 2.2.2.2 37 0x80000004 0xac3c 1
```

```
Network-LSA (Area 0.0.0.1)
Link State ID ADV Router Age Seq# CkSum
0.0.0.1 2.2.2.2 42 0x80000001 0x21d2
```

```
Inter-Area-Prefix-LSA (Area 0.0.0.1)
Link State ID ADV Router Age Seq# CkSum Prefix
0.0.0.1 2.2.2.2 42 0x80000004 0xbc0a 2001:2::/64
0.0.0.4 2.2.2.2 19 0x80000001 0xb80c 2001:3::/64
0.0.0.5 2.2.2.2 19 0x80000001 0xd0ef 2001:5::/64
```

```
Intra-Area-Prefix-LSA (Area 0.0.0.1)
Link State ID ADV Router Age Seq# CkSum Prefix Reference
0.0.0.1 1.1.1.1 35 0x80000005 0xc4ce 1 Router-LSA
0.0.0.3 2.2.2.2 41 0x80000001 0x8807 1 Network-LSA
```

For Device2, both 2001:3::/642 and 2001:5::/64 are inter-area routes. Relevant routing LSA information can be seen from Inter-Area-Prefix-LSA (Area 0.0.0.0). For intra-area route, show ipv6 ospf database intra-prefix is required to see relevant routing LSA information.

Step 4: Configure the network type of OSPFv3 interface as point-to-point.

#On Device3, change the OSPFv3 network type of vlan3 to point-to-point.

```
Device3(config)#interface vlan3
Device3(config-if-vlan3)#ipv6 ospf network point-to-point
Device3(config-if-vlan3)#exit
```

#On Device4, change the OSPFv3 network type of vlan2 to point-to-point.

```
Device4(config)#interface vlan2
Device4(config-if-vlan2)#ipv6 ospf network point-to-point
Device4(config-if-vlan2)#exit
```

Step 5: Check the result.

#View the OSPFv3 neighbors and routing table on Device3.

```
Device3#show ipv6 ospf neighbor
OSPFv3 Process (100)
Neighbor ID Pri State Dead Time Interface Instance ID
2.2.2.2 1 Full/Backup 00:00:39 vlan2 0
4.4.4.4 1 Full/- 00:00:39 vlan3 0
```

```
Device3#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
U - Per-user Static route
O - OSPF, OE-OSPF External, M - Management
```

```
L ::1/128 [0/0]
via ::, 1d:09:10:10, lo0
O 2001:1::/64 [110/2]
via fe80::201:7aff:fe5e:6d46, 02:07:25, vlan2
C 2001:2::/64 [0/0]
via ::, 03:07:51, vlan2
L 2001:2::2/128 [0/0]
via ::, 03:07:48, lo0
C 2001:3::/64 [0/0]
via ::, 03:07:41, vlan3
L 2001:3::1/128 [0/0]
```

```
via ::, 03:07:39, lo0
O 2001:4::/64 [110/3]
via fe80::201:7aff:fe5e:6d46, 02:07:25, vlan2
O 2001:5::/64 [110/2]
via fe80::201:2ff:fe03:405, 00:00:22, vlan3
```

---

## Note

- When OSPFv3 neighbor relations are established in point-to-point networks, there is no DR or BDR election.
- 

#View the OSPFv3 neighbors and routing table on Device4.

```
Device4#show ipv6 ospf neighbor
OSPFv3 Process (100)
Neighbor ID  Pri  State      Dead Time  Interface          Instance ID
3.3.3.3      1  Full/-    00:00:38  vlan2              0

Device4#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
via ::, 00:05:34, lo0
O 2001:1::/64 [110/3]
via fe80::2212:1ff:fe01:102, 00:03:12, vlan2
O 2001:2::/64 [110/2]
via fe80::2212:1ff:fe01:102, 00:03:12, vlan2
C 2001:3::/64 [0/0]
via ::, 00:04:34, vlan2
L 2001:3::2/128 [0/0]
via ::, 00:04:31, lo0
O 2001:4::/64 [110/4]
via fe80::2212:1ff:fe01:102, 00:03:12, vlan2
C 2001:5::/64 [0/0]
via ::, 00:03:14, vlan3
L 2001:5::1/128 [0/0]
via ::, 00:03:13, lo0
```

According to the result, after the network type of OSPFv3 interface is changed to point-to-point, neighbors can be normally established, and routes can be learned normally.

## 56.3.2 Configure OSPFv3 to use IPSec encryption & authentication

### Network Requirements

- All routers run OSPFv3, and the entire AS is divided into 2 areas.
- Device1, Device2, and Device3 use IPSec tunnels to encrypt and authenticate OSPFv3 protocol packets. Device1 and Device2 adopt ESP transmission and encapsulation, with the encryption algorithm being 3des and authentication algorithm sha1. Device2 and Device3 also use ESP transmission and encapsulation, but the encryption algorithm is aes128 and ESP authentication algorithm is sm3.

- Upon completion of the configuration, the device can normally establish neighbors and learn routes from each other.

### Network Topology

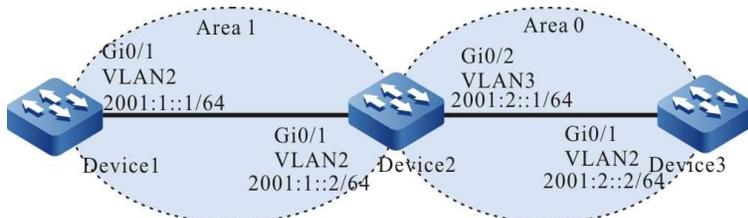


Figure 56 Network Topology for Configuring OSPFv3 to Use IPsec Encryption & Authentication

### Configuration Steps

Step 1: Configure IPv6 addresses for the ports. (Omitted)

Step 2: Configure OSPFv3 process and enable OSPFv3 function on corresponding interface.

#On Device1, Device2 and Device3, configure OSPFv3 process and enable OSPFv3 on the interface.

```
Device1#configure terminal
Device1(config)#ipv6 router ospf 100
Device1(config-ospf6)#router-id 1.1.1.1
Device1(config-ospf6)#exit
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ipv6 router ospf 100 area 1
Device1(config-if-vlan2)#exit

Device2#configure terminal
Device2(config)#ipv6 router ospf 100
Device2(config-ospf6)#router-id 2.2.2.2
Device2(config-ospf6)#exit
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ipv6 router ospf 100 area 1
Device2(config-if-vlan2)#exit
Device2(config)#interface vlan3
Device2(config-if-vlan3)#ipv6 router ospf 100 area 0
Device2(config-if-vlan3)#exit

Device3#configure terminal
Device3(config)#ipv6 router ospf 100
Device3(config-ospf6)#router-id 3.3.3.3
Device3(config-ospf6)#exit
Device3(config)#interface vlan2
Device3(config-if-vlan2)#ipv6 router ospf 100 area 0
Device3(config-if-vlan2)#exit
```

Step 3: Configure IPsec proposal and manual tunnel.

#On Device1, create IPsec proposal a, use ESP transmission & encapsulation mode (encryption algorithm 3des, authentication algorithm sha1), create IPsec manual tunnel a, and configure SPI and key.

```
Device1(config)#crypto ipsec proposal a
Device1(config-ipsec-prop)#mode transport
Device1(config-ipsec-prop)#esp 3des sha1
```



```
Device2(config-ospf6)#area 0 ipsec-tunnel b
Device1(config-ospf6)#exit
```

#In the OSPFv3 process of Device3, bind IPsec tunnel b to area 0.

```
Device3(config)#ipv6 router ospf 100
Device3(config-ospf6)#area 0 ipsec-tunnel b
Device3(config-ospf6)#exit
```

Step 5: Check the result.

#View OSPFv3 process information on Device1.

```
Device1#show ipv6 ospf 100
Routing Process "OSPFv3 (100)" with ID 1.1.1.1
Process bound to VRF default
IETF graceful-restarter support disabled
IETF gr helper support enabled
Initial SPF schedule delay 5000 msec
Minimum hold time between two consecutive SPF's 10000 msec
Maximum wait time between two consecutive SPF's 10000 msec
Minimum LSA interval 5 secs, Minimum LSA arrival 1 secs
Number of external LSA 0. Checksum Sum 0x0000
Number of AS-Scoped Unknown LSA 0
Number of LSA originated 5
Number of LSA received 5
Number of areas in this router is 1
Not Support Demand Circuit lsa number is 0
Autonomy system support flood DoNotAge Lsa
Area 0.0.0.1
Number of interfaces in this area is 1
IPSec Tunnel Name:a , ID: 154
Number of fully adjacent neighbors in this area is 1
Number of fully adjacent sham-link neighbors in this area is 0
Number of fully adjacent virtual neighbors through this area is 0
SPF algorithm executed 4 times
LSA walker due in 00:00:02
Number of LSA 4. Checksum Sum 0x2FC53
Number of Unknown LSA 0
Not Support Demand Circuit lsa number is 0
Indication lsa (by other routers) number is: 0,
area support flood DoNotAge Lsa
```

According to the result, IPsec tunnel a has been bound to the area, and ID is the random value in 0~1023.

#View IPsec tunnel information on Device1.

```
Device1# show crypto ipv6-tunnel a
get the manual ipv6 tunnel
Crypto tunnelv6 a : MANUAL
policy name : (null)
peer address :
local interface : (null) address :
Ipssec proposal : a
Inbound :
  esp : spi: 1000 encryption key: ***** authentication key: *****
  ah spi: 0 authentication key: (null)
Outbound :
  esp spi: 1001 encryption key: ***** authentication key: *****
  ah spi: 0 authentication key: (null)
route ref : 1
route asyn : 1
route rt_id : 154
```

According to the result, the IDs in route rt\_id and show ipv6 ospf 100 are equal.

#View IPsec tunnel encryption type on Device1.

```
Device1# show crypto ipsec sa ipv6-tunnel a
```

```

route policy:
the pairs of ESP ipsec sa : id :0 , algorithm : 3DES HMAC-SHA1-96
inbound esp ipsec sa : spi : 0x3e8(1000) crypto m_context(s_context) : 0x4cd3ba78 / 0x4cd3bae0
  current input 26 packets, 2 kbytes
  encapsulation mode : Transport
  replay protection : OFF
  remaining lifetime (seconds/kbytes) : 0/0
  uptime is 0 hour 4 minute 45 second
outbound esp ipsec sa : spi : 0x3e9(1001) crypto m_context(s_context) : 0x4cd3bb48 / 0x4cd3bbb0
  current output 39 packets, 3 kbytes
  encapsulation mode : Transport
  replay protection : OFF
  remaining lifetime (seconds/kbytes) : 0/0
  uptime is 0 hour 4 minute 45 second

```

total sa and sa group is 1

According to the result, IPSec tunnel a adopts ESP transmission & encryption mode, with the encryption algorithm being 3des and authentication algorithm sha1.

#View OSPFv3 interface information on Device1.

```

Device1#show ipv6 ospf interface vlan2
vlan2 is up, line protocol is up
Interface ID 50331913
IPv6 Prefixes
fe80::201:7aff:fe9:fbec/10 (Link-Local Address)
2001::1::1/64
Interface ID 13
OSPFv3 Process (100), Area 0.0.0.1, Instance ID 0, Enabled 00:41:10, MTU 1500
Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
IPSec tunnel(Area):a, ID:154
Transmit Delay is 1 sec, State Backup, 3 state change, Priority 1
Designated Router (ID) 2.2.2.2
  Interface Address fe80::200:1ff:fe7a:adf0
Backup Designated Router (ID) 1.1.1.1
  Interface Address fe80::201:7aff:fe9:fbec
Timer interval configured, Hello 10, Dead 39, Wait 39, Retransmit 5
Hello due in 00:00:06
Neighbor Count is 1, Adjacent neighbor count is 1
Hello received 2 sent 3, DD received 3 sent 4
LS-Req received 1 sent 1, LS-Upd received 5 sent 3
LS-Ack received 3 sent 2, Discarded 0

```

According to the result, IPSec tunnel a has been bound to the interface, and ID is the random value in 0~1023.

#View OSPFv3 neighbors' information and core routing table on Device1.

```

Device1#show ipv6 ospf neighbor
OSPFv3 Process (100)
Neighbor ID  Pri  State    Dead Time  Interface        Instance ID
2.2.2.2      1   Full/DR  00:00:39   vlan2            0

```

```

Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
U - Per-user Static route
O - OSPF, OE-OSPF External, M - Management

```

```

L ::1/128 [0/0]
  via ::, 4d:04:06:36, lo0
C 2001:1::/64 [0/0]
  via ::, 03:00:53, vlan2
L 2001:1::1/128 [0/0]
  via ::, 03:00:49, lo0
O 2001:2::/64 [110/2]
  via fe80::201:7aff:fe9:1cdd, 2d:00:03:49, vlan2

```

On Device1, neighbors are normally established, and route learning is normal.

### #View OSPFv3 process information on Device3.

```
Device3#show ipv6 ospf 100
Routing Process "OSPFv3 (100)" with ID 3.3.3.3
Process bound to VRF default
IETF graceful-restarter support disabled
IETF gr helper support enabled
Initial SPF schedule delay 5000 msec
Minimum hold time between two consecutive SPF's 10000 msec
Maximum wait time between two consecutive SPF's 10000 msec
Minimum LSA interval 5 secs, Minimum LSA arrival 1 secs
Number of external LSA 0. Checksum Sum 0x0000
Number of AS-Scoped Unknown LSA 0
Number of LSA originated 5
Number of LSA received 6
Number of areas in this router is 1
Not Support Demand Circuit lsa number is 0
Autonomy system support flood DoNotAge Lsa
Area BACKBONE(0)
  Number of interfaces in this area is 1
  IPsec Tunnel Name:b , ID: 2
  Number of fully adjacent neighbors in this area is 1
  Number of fully adjacent sham-link neighbors in this area is 0
  SPF algorithm executed 4 times
  LSA walker due in 00:00:02
  Number of LSA 4. Checksum Sum 0x24272
  Number of Unknown LSA 0
  Not Support Demand Circuit lsa number is 0
  Indication lsa (by other routers) number is: 0,
  area support flood DoNotAge Lsa
```

According to the result, IPsec tunnel b has been bound to the area, and ID is the random value in 0~1023.

### #View information about IPsec tunnel of Device3.

```
Device3# show crypto ipv6-tunnel b
get the manual ipv6 tunnel
Crypto tunnelv6 a : MANUAL
  policy name : (null)
  peer address :
  local interface : (null) address :
  Ipsec proposal : b
  Inbound :
    esp spi: 2000 encryption key: ***** authentication key: *****
    ah spi: 0 authentication key: (null)
  Outbound :
    esp spi: 2001 encryption key: ***** authentication key: *****
    ah spi: 0 authentication key: (null)
  route ref : 1
  route asyn : 1
  route rt_id : 2
```

According to the result, the IDs in route rt\_id and show ipv6 ospf 100 are equal.

### #View IPsec tunnel encryption type on Device3.

```
Device3# show crypto ipsec sa ipv6-tunnel b
route policy:
  the pairs of ESP ipsec sa : id : 0, algorithm : AES128 HMAC-SM3
inbound esp ipsec sa : spi : 0x7d0(2000) crypto m_context(s_context) : 0x6a0d9a98 /
0x6a0d9a30
  current input 53 packets, 5 kbytes
  encapsulation mode : Transport
  replay protection : OFF
  remaining lifetime (seconds/kbytes) : 0/0
  uptime is 0 hour 6 minute 40 second
outbound esp ipsec sa : spi : 0x7d1(2001) crypto m_context(s_context) : 0x6a0d99c8 /
0x6a0d9960
  current output 52 packets, 5 kbytes
  encapsulation mode : Transport
```

```
replay protection : OFF
remaining lifetime (seconds/kbytes) : 0/0
uptime is 0 hour 6 minute 40 second
```

```
total sa and sa group is 1
```

According to the result, IPsec tunnel adopts ESP transmission & encryption mode, with the encryption algorithm being aes128 and authentication algorithm sm3.

```
#View OSPFv3 interface information on Device3.
Device3#show ipv6 ospf interface vlan2
vlan2 is up, line protocol is up
Interface ID 50331899
IPv6 Prefixes
 fe80::200:1ff:fe7a:adf0/10 (Link-Local Address)
 2001::2::1/64
Interface ID 9
OSPFv3 Process (100), Area 0.0.0.1, Instance ID 0, Enabled 00:50:39, MTU 1500
Router ID 3.3.3.3, Network Type BROADCAST, Cost: 1
  IPsec tunnel(Area):b, ID:2
Transmit Delay is 1 sec, State DR, 4 state change, Priority 1
Designated Router (ID) 2.2.2.2
 Interface Address fe80::200:1ff:fe7a:adf0
Backup Designated Router (ID) 1.1.1.1
 Interface Address fe80::201:7aff:fecf:fbec
Timer interval configured, Hello 10, Dead 39, Wait 39, Retransmit 5
Hello due in 00:00:02
Neighbor Count is 1, Adjacent neighbor count is 1
Hello received 272 sent 316, DD received 12 sent 9
LS-Req received 3 sent 5, LS-Upd received 19 sent 18
LS-Ack received 11 sent 13, Discarded 0
```

According to the result, IPsec tunnel b has been bound to the interface, and ID is the random value in 0~1023.

#View OSPFv3 neighbors' information and core routing table on Device3.

```
Device3#show ipv6 ospf neighbor
OSPFv3 Process (100)
Neighbor ID  Pri  State  Dead Time  Interface  Instance ID
2.2.2.2      1    Full/Backup  00:00:35   vlan2  0

Device3#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L  ::1/128 [0/0]
   via ::, 09:53:53, lo0
O  2001:1::/64 [110/2]
   via fe80::ae9c:e4ff:fe77:889e, 00:23:36, vlan2
C  2001:2::/64 [0/0]
   via ::, 03:05:16, vlan2
L  2001:2::2/128 [0/0]
   via ::, 03:05:13, lo0
```

On Device3, neighbors are normally established, and route learning is normal.

Step 6: Bind corresponding IPsec tunnel to the OSPFv3 interface.

#On Device1, bind IPsec tunnel a to Vlan2.

```
Device1(config)#interface vlan2
Device1(config-if- vlan2)#ipv6 ospf ipsec-tunnel a
Device1(config-if- vlan2)#exit
```

#On Device2, bind IPsec tunnel a to vlan2 and IPsec tunnel b to vlan3.

```
Device2(config)#interface vlan2
Device2(config-if- vlan2)#ipv6 ospf ipsec-tunnel a
Device2(config-if- vlan2)#exit
Device2(config)#interface vlan3
Device2(config-if-vlan3)#ipv6 ospf ipsec-tunnel b
Device2(config-if-vlan3)#exit
```

#On Device3, bind IPsec tunnel b to vlan2.

```
Device3(config)#interface vlan2
Device3(config-if- vlan2)#ipv6 ospf ipsec-tunnel b
Device3(config-if- vlan2)#exit
```

Step 7: Check the result.

#View OSPFv3 interface information on Device1.

```
Device1#show ipv6 ospf interface vlan2
vlan2 is up, line protocol is up
Interface ID 50331913
IPv6 Prefixes
  fe80::201:7aff:fe7a:adf0 (Link-Local Address)
  2001::1::1/64
Interface ID 13
OSPFv3 Process (100), Area 0.0.0.1, Instance ID 0, Enabled 00:41:10, MTU 1500
Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
  IPsec tunnel:a, ID:154
Transmit Delay is 1 sec, State Backup, 3 state change, Priority 1
Designated Router (ID) 2.2.2.2
  Interface Address fe80::200:1ff:fe7a:adf0
Backup Designated Router (ID) 1.1.1.1
  Interface Address fe80::201:7aff:fe7a:adf0
Timer interval configured, Hello 10, Dead 39, Retransmit 5
Hello due in 00:00:06
Neighbor Count is 1, Adjacent neighbor count is 1
Hello received 2 sent 3, DD received 3 sent 4
LS-Req received 1 sent 1, LS-Upd received 5 sent 3
LS-Ack received 3 sent 2, Discarded 0
```

According to the result, IPsec tunnel a has been bound to the interface, and ID is the random value in 0~1023.

#View the core routing table of OSPFv3 on Device1.

```
Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
  via ::, 4d:04:06:36, lo0
C 2001::1::/64 [0/0]
  via ::, 03:00:53, vlan2
L 2001::1::/128 [0/0]
  via ::, 03:00:49, lo0
O 2001::2::/64 [110/2]
  via fe80::201:7aff:fe7a:adf0, 2d:00:03:49, vlan2
```

On Device1, route learning is normal.

#View OSPFv3 interface information on Device3.

```
Device3#show ipv6 ospf interface vlan2
vlan2 is up, line protocol is up
```

```

Interface ID 50331899
IPv6 Prefixes
 fe80::200:1ff:fe7a:adf0/10 (Link-Local Address)
 2001:2::1/64
Interface ID 9
OSPFv3 Process (100), Area 0.0.0.1, Instance ID 0, Enabled 00:50:39, MTU 1500
Router ID 3.3.3.3, Network Type BROADCAST, Cost: 1
IPSec tunnel:b, ID:2
Transmit Delay is 1 sec, State DR, 4 state change, Priority 1
Designated Router (ID) 2.2.2.2
Interface Address fe80::200:1ff:fe7a:adf0
Backup Designated Router (ID) 1.1.1.1
Interface Address fe80::201:7aff:fecf:fbec
Timer interval configured, Hello 10, Dead 39, Wait 39, Retransmit 5
Hello due in 00:00:02
Neighbor Count is 1, Adjacent neighbor count is 1
Hello received 272 sent 316, DD received 12 sent 9
LS-Req received 3 sent 5, LS-Upd received 19 sent 18
LS-Ack received 11 sent 13, Discarded 0

```

According to the result, IPSec tunnel b has been bound to the interface, and ID is the random value in 0~1023.

#View the core routing table of OSPFv3 on Device3.

```

Device3#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
  via ::, 09:53:53, lo0
O 2001:1::/64 [110/2]
  via fe80::ae9c:e4ff:fe77:889e, 00:23:36, vlan2
C 2001:2::/64 [0/0]
  via ::, 03:05:16, vlan2
L 2001:2::2/128 [0/0]
  via ::, 03:05:13, lo0

```

On Device3, route learning is normal.

---

### Note

- When configuring OSPFv3 to bind an IPSec tunnel, you can configure area binding or interface binding only, or configure both area and interface binding.
  - When IPSec tunnel is configured for area binding and interface binding at the same time, the latter takes effect first.
- 

## 56.3.3 Configure coordination of OSPFv3 with BFD

### Network Requirements

- All devices are configured with OSPFv3 protocol.
- Enable BFD detection function for the lines between Device1 and Device3. When the lines fail, BFD will quickly identify these failures and notify OSPFv3 which will switch route to Device2 for communication.

## Network Topology

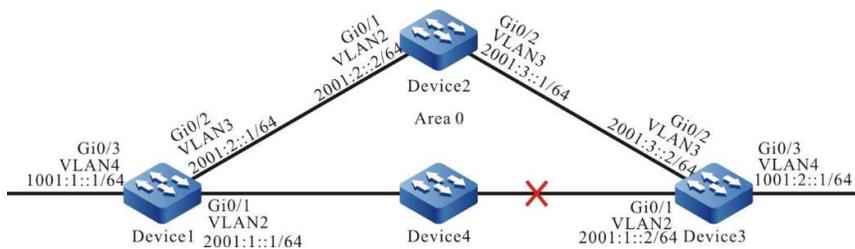


Figure 56 Network Topology for Configuring Coordination of OSPFv3 with BFD

### Configuration Steps

Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configure IPv6 addresses for the ports. (Omitted)

Step 3: Configure OSPFv3 process.

#### #Configure Device1.

```
Device1#configure terminal
Device1(config)#ipv6 router ospf 100
Device1(config-ospf6)#router-id 1.1.1.1
Device1(config-ospf6)#exit
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ipv6 router ospf 100 area 0
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan3
Device1(config-if-vlan3)#ipv6 router ospf 100 area 0
Device1(config-if-vlan3)#exit
Device1(config)#interface vlan4
Device1(config-if-vlan4)#ipv6 router ospf 100 area 0
Device1(config-if-vlan4)#exit
```

#### #Configure Device2.

```
Device2#configure terminal
Device2(config)#ipv6 router ospf 100
Device2(config-ospf6)#router-id 2.2.2.2
Device2(config-ospf6)#exit
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ipv6 router ospf 100 area 0
Device2(config-if-vlan2)#exit
Device2(config)#interface vlan3
Device2(config-if-vlan3)#ipv6 router ospf 100 area 0
Device2(config-if-vlan3)#exit
```

#### #Configure Device3.

```
Device3#configure terminal
Device3(config)#ipv6 router ospf 100
Device3(config-ospf6)#router-id 3.3.3.3
Device3(config-ospf6)#exit
Device3(config)#interface vlan2
Device3(config-if-vlan2)#ipv6 router ospf 100 area 0
Device3(config-if-vlan2)#exit
Device3(config)#interface vlan3
Device3(config-if-vlan3)#ipv6 router ospf 100 area 0
Device3(config-if-vlan3)#exit
```

```
Device3(config)#interface vlan4
Device3(config-if-vlan4)#ipv6 router ospf 100 area 0
Device3(config-if-vlan4)#exit
```

Step 4: Configure coordination of OSPFv3 with BFD.

#Configure Device1.

```
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ipv6 ospf bfd
Device1(config-if-vlan2)#exit
```

#Configure Device3.

```
Device3(config)#interface vlan2
Device3(config-if-vlan2)#ipv6 ospf bfd
Device3(config-if-vlan2)#exit
```

Step 5: Check the result.

#View OSPFv3 neighbors' information and routing table on Device1.

```
Device1#show ipv6 ospf neighbor 3.3.3.3
OSPFv3 Process (100)

Neighbor 3.3.3.3,interface address fe80::2212:1ff:fe01:104
  In the area 0.0.0.0 via interface vlan4, BFD enabled
  DR is 3.3.3.3 BDR is 1.1.1.1
  Neighbor priority is 1, State is Full, 6 state changes
  Options is 0x13 (-R|-|E|V6)
  Dead timer due in 00:00:37
  Neighbor is up for 00:01:31
  Database Summary List 0
  Link State Request List 0
  Link State Retransmission List 0
  Thread Inactivity Timer on
  Thread Database Description Retransmission off, 0 times
  Thread Link State Request Retransmission off, 0 times
  Thread Link State Update Retransmission off, 0 times

Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
  via ::, 01:15:27, lo0
C 1001:1::/64 [0/0]
  via ::, 01:15:27, vlan4
L 1001:1::1/128 [0/0]
  via ::, 01:15:27, lo0
O 1001:2::/64 [110/2]
  via fe80::2212:1ff:fe01:104, 00:02:40, vlan2
C 2001:1::/64 [0/0]
  via ::, 01:15:27, vlan2
L 2001:1::1/128 [0/0]
  via ::, 01:15:27, lo0
C 2001:2::/64 [0/0]
  via ::, 01:15:27, vlan3
L 2001:2::1/128 [0/0]
  via ::, 01:15:27, lo0
O 2001:3::/64 [110/2]
  via fe80::201:7aff:fe5e:6d45, 00:02:40, vlan3
  [110/2]
  via fe80::2212:1ff:fe01:104, 00:02:40, vlan2
```

According to the information of OSPFv3 neighbors, BFD has been enabled, and the route 1001:2::/64 prefers the lines between Device1 and Device3 for communication.

#View the BFD session information of Device1.

```
Device1#show bfd session ipv6 detail
Total ipv6 session number: 1
OurAddr          NeighAddr          State  Holddown  Interface
fe80::201:7aff:fe61:7a25  fe80::2212:1ff:fe01:104  UP     5000     vlan2
Type:ipv6 direct
Local State:UP Remote State:UP Up for: 0h:0m:4s Number of times UP:1
Local Discriminator:5 Remote Discriminator:95
Send Interval:1000ms Detection time:5000ms(1000ms*5)
Local Diag:0 Demand mode:0 Poll bit:0
MinTxInt:1000 MinRxInt:1000 Multiplier:5
Remote MinTxInt:1000 Remote MinRxInt:1000 Remote Multiplier:5
Registered modules:OSPFv3
```

According to the result, OSPFv3 has been successfully coordinated with BFD, and the session is established normally.

#When the lines between Device1 and Device3 fail, BFD can quickly identify these failures and notify OSPFv3 which will switch route to Device2 for communication and view the routing table on Device1.

```
Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
  via ::, 01:16:10, lo0
C 1001:1::/64 [0/0]
  via ::, 01:16:10, vlan4
L 1001:1::/128 [0/0]
  via ::, 01:16:10, lo0
O 1001:2::/64 [110/3]
  via fe80::201:7aff:fe5e:6d45, 00:00:07, vlan3
C 2001:1::/64 [0/0]
  via ::, 01:16:10, vlan2
L 2001:1::/128 [0/0]
  via ::, 01:16:10, lo0
C 2001:2::/64 [0/0]
  via ::, 01:16:10, vlan3
L 2001:2::/128 [0/0]
  via ::, 01:16:10, lo0
O 2001:3::/64 [110/2]
  via fe80::201:7aff:fe5e:6d45, 00:03:22, vlan3
```

Device3 has similar behaviors to Device1.

### 56.3.4 Configure OSPFv3 static FRR

#### Network Requirements

- All devices are configured with OSPFv3 protocol.
- Enable static FRR between Device1 and Device3. When the lines fail, the service can quickly switch to Device2 for communication.

#### Network Topology

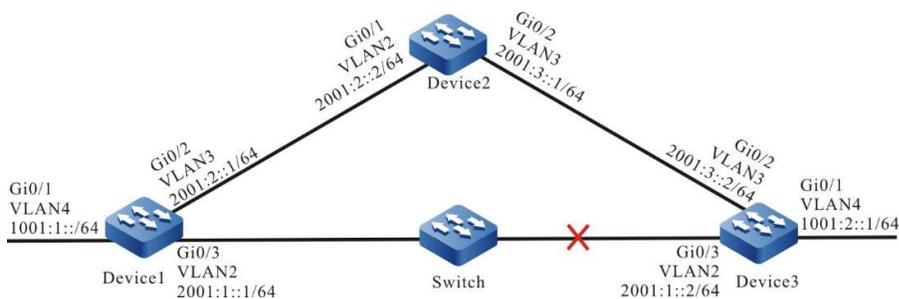


Figure 1 Network Topology for Configuring OSPFv3 Static FRR

### Configuration Steps

Step 1: Configure VLAN, and add ports to the required VLAN; configure the IPv6 address of each interface (Omitted).

Step 2: Configure OSPFv3 process.

#### #Configure Device1.

```
Device1#configure terminal
Device1(config)#ipv6 router ospf 100
Device1(config-ospf6)#router-id 1.1.1.1
Device1(config-ospf6)#exit
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ipv6 router ospf 100 area 0
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan3
Device1(config-if-vlan3)#ipv6 router ospf 100 area 0
Device1(config-if-vlan3)#exit
```

#### #Configure Device2.

```
Device2#configure terminal
Device2(config)#ipv6 router ospf 100
Device2(config-ospf6)#router-id 2.2.2.2
Device2(config-ospf6)#exit
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ipv6 router ospf 100 area 0
Device2(config-if-vlan2)#exit
Device2(config)#interface vlan3
Device2(config-if-vlan3)#ipv6 router ospf 100 area 0
Device2(config-if-vlan3)#exit
```

#### #Configure Device3.

```
Device3#configure terminal
Device3(config)#ipv6 router ospf 100
Device3(config-ospf6)#router-id 3.3.3.3
Device3(config-ospf6)#exit
Device3(config)#interface vlan2
Device3(config-if-vlan2)#ipv6 router ospf 100 area 0
Device3(config-if-vlan2)#exit
Device3(config)#interface vlan3
Device3(config-if-vlan3)#ipv6 router ospf 100 area 0
Device3(config-if-vlan3)#exit
Device3(config)#interface vlan4
Device3(config-if-vlan4)#ipv6 router ospf 100 area 0
Device3(config-if-vlan4)#exit
```

Step 3: Configure routing policy.

#On Device1, configure route-map to invoke ACL to match 1001:2::1/64 only, and filter other network segments. The route matching the match rule applies the backup next hop interface vlan3. The next hop address is 2001:2::2.

```
Device1(config)#ipv6 access-list extended 7001
Device1(config-v6-list)#permit ipv6 1001:2::1/64 any
Device1(config-v6-list)#exit
Device1(config)#route-map ipv6frr_ospf
Device1(config-route-map)#match ipv6 address 7001
Device1(config-route-map)#set ipv6 fast-reroute backup-interface vlan3 backup-next-hop 2001:2::2
Device1(config-route-map)#exit
```

Step 4: Configure static FRR.

```
Device1(config)#ipv6 router ospf 100
Device1(config-ospf6)#fast-reroute route-map ipv6frr_ospf
Device1(config-ospf6)#exit
```

Step 5: Check the results.

#View OSPFv3 routing table on Device1.

```
Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management
L ::1/128 [0/0]
  via ::, 00:31:05, lo0
C 1001:1::/64 [0/0]
  via ::, 00:26:12, vlan4
L 1001:1::1/128 [0/0]
  via ::, 00:26:12, vlan4
O 1001:2::/64 [110/2]
  via fe80::201:7aff:fe92:e6b6, 00:22:11, vlan2
C 2001:1::/64 [0/0]
  via ::, 00:26:51, vlan2
L 2001:1::1/128 [0/0]
  via ::, 00:26:51, vlan2
C 2001:2::/64 [0/0]
  via ::, 00:25:30, vlan3
L 2001:2::1/128 [0/0]
  via ::, 00:25:30, vlan3
O 2001:3::/64 [110/2]
  via fe80::201:7aff:fe92:e6b6, 00:20:53, vlan2
  via fe80::ced8:1fff:fe10:7aae, 00:21:06, vlan3
```

According to the routing table, the route 1001:2::/64 prefers the lines between Device1 and Device3 for communication.

#View IPv6 FRR routing table on Device1.

```
Device1#show ipv6 frr route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management
O 1001:2::/64 [110/4294967295]
  via 2001:2::2, 00:03:16, vlan3
```

According to the result, the next hop and output interface of the frr route 1001:2::/64 are 2001:2::2 and vlan3 respectively.

#View the BFD session information of Device1.

```
Device1#show bfd session ipv6 2001:1::1 detail
Total ipv6 session number: 1
OurAddr      NeighAddr  LD/RD      State  Holddown  Interface
2001:1::1    2001:1::1  1017/1017  UP     500       vlan2
Type:ipv6 direct Mode:echo
Local Discriminator:65 Remote Discriminator:65
Local State:UP Remote State:UP Up for: 0h:9m:11s Number of times UP:1
Send Interval:100ms Detection time:500ms(100ms*5)
Local Diag:0 Demand mode:0 Poll bit:0
Registered modules:FIB_MGR
```

According to the result, FIB\_MGR has been successfully coordinated with BFD. The session is established normally in the mode of echo.

#When the lines between Device1 and Device3 fail, it can quickly identify the failures and switch to Device2 for communication. The routing table of Device1 shows that the output interface of the destination network 1001:2::/64 has switched to the backup interface vlan3.

```
Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management
L ::1/128 [0/0]
  via ::, 03:03:45, lo0
C 1001:1::/64 [0/0]
  via ::, 02:58:52, vlan4
L 1001:1::1/128 [0/0]
  via ::, 02:58:52, vlan4
O 1001:2::/64 [110/3]
  via fe80::ced8:1fff:fe10:7aae, 00:00:11, vlan3
C 2001:1::/64 [0/0]
  via ::, 02:59:31, vlan2
L 2001:1::1/128 [0/0]
  via ::, 02:59:31, vlan2
C 2001:2::/64 [0/0]
  via ::, 02:58:10, vlan3
L 2001:2::1/128 [0/0]
  via ::, 02:58:10, vlan3
O 2001:3::/64 [110/2]
  via fe80::ced8:1fff:fe10:7aae, 02:53:45, vlan3
```

### 56.3.5 Configure OSPFv3 dynamic FRR

#### Network Requirements

- All devices are configured with OSPFv3 protocol.
- Enable dynamic FRR between Device1 and Device3. When the lines fail, the service can quickly switch to Device2 for communication.

#### Network Topology

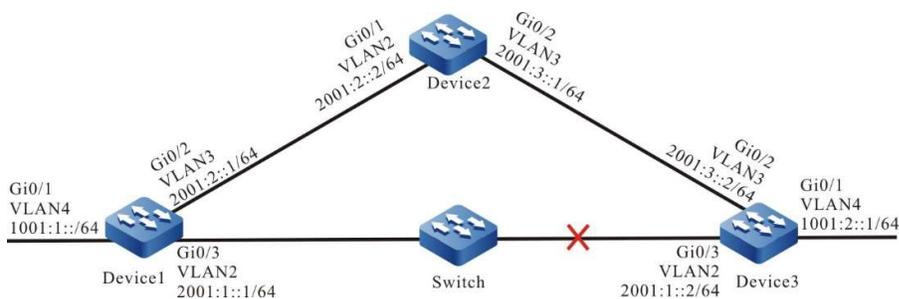


Figure 2 Network Topology for Configuring OSPFv3 Dynamic FRR

### Configuration Steps

- Step 1: Configure VLAN, and add ports to the required VLAN; configure the IPv6 address of each interface (Omitted).
- Step 2: Configure OSPFv3 process and the network type of interface as point-to-point.

#### #Configure Device1.

```
Device1#configure terminal
Device1(config)#ipv6 router ospf 100
Device1(config-ospf6)#router-id 1.1.1.1
Device1(config-ospf6)#exit
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ipv6 router ospf 100 area 0
Device1(config-if-vlan2)# ipv6 ospf network point-to-point
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan3
Device1(config-if-vlan3)#ipv6 router ospf 100 area 0
Device1(config-if-vlan3)# ipv6 ospf network point-to-point
Device1(config-if-vlan3)#exit
```

#### #Configure Device2.

```
Device2#configure terminal
Device2(config)#ipv6 router ospf 100
Device2(config-ospf6)#router-id 2.2.2.2
Device2(config-ospf6)#exit
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ipv6 router ospf 100 area 0
Device2(config-if-vlan2)# ipv6 ospf network point-to-point
Device2(config-if-vlan2)#exit
Device2(config)#interface vlan3
Device2(config-if-vlan3)#ipv6 router ospf 100 area 0
Device2(config-if-vlan3)# ipv6 ospf network point-to-point
Device2(config-if-vlan3)#exit
```

#### #Configure Device3.

```
Device3#configure terminal
Device3(config)#ipv6 router ospf 100
Device3(config-ospf6)#router-id 3.3.3.3
Device3(config-ospf6)#exit
Device3(config)#interface vlan2
Device3(config-if-vlan2)#ipv6 router ospf 100 area 0
Device3(config-if-vlan2)# ipv6 ospf network point-to-point
Device3(config-if-vlan2)#exit
Device3(config)#interface vlan3
Device3(config-if-vlan3)#ipv6 router ospf 100 area 0
Device3(config-if-vlan3)# ipv6 ospf network point-to-point
Device3(config-if-vlan3)#exit
```

```

Device3(config)#interface vlan4
Device3(config-if-vlan4)#ipv6 router ospf 100 area 0
Device3(config-if-vlan4)# ipv6 ospf network point-to-point
Device3(config-if-vlan4)#exit

```

Step 3: Configure routing policy.

#On Device1, configure route-map to invoke ACL to match 1001:2::1/64 only, and filter other network segments.

```

Device1(config)#ipv6 access-list extended 7001
Device1(config-v6-list)#permit ipv6 1001:2::1/64 any
Device1(config-v6-list)#exit
Device1(config)#route-map ipv6frr_ospf
Device1(config-route-map)#match ipv6 address 7001
Device1(config-route-map)#exit

```

Step 4: Configure dynamic FRR.

```

Device1(config)#ipv6 router ospf 100
Device1(config-ospf6)# fast-reroute loop-free-alternate route-map ipv6frr_ospf
Device1(config-ospf6)#exit

```

Step 5: Check the results.

#View OSPFv3 routing table on Device1.

```

Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management
L ::1/128 [0/0]
  via ::, 03:21:35, lo0
C 1001:1::/64 [0/0]
  via ::, 03:16:42, vlan4
L 1001:1::1/128 [0/0]
  via ::, 03:16:42, vlan4
O 1001:2::/64 [110/2]
  via fe80::201:7aff:fe92:e6b6, 00:01:35, vlan2
C 2001:1::/64 [0/0]
  via ::, 03:17:21, vlan2
L 2001:1::1/128 [0/0]
  via ::, 03:17:21, vlan2
C 2001:2::/64 [0/0]
  via ::, 03:16:00, vlan3
L 2001:2::1/128 [0/0]
  via ::, 03:16:00, vlan3
O 2001:3::/64 [110/2]
  via fe80::ced8:1fff:fe10:7aae, 00:07:50, vlan3

```

According to the routing table, the route 1001:2::/64 prefers the lines between Device1 and Device3 for communication.

#View IPv6 FRR routing table on Device1.

```

Device1#show ipv6 frr route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management
O 1001:2::/64 [110/4294967295]
  via fe80::ced8:1fff:fe10:7aae, 00:01:58, vlan3

```

According to the result, the next hop of FRR route 1001:2::/64 is the linklocal address fe80::ced8:1fff:fe10:7aae, and the output interface is vlan3.

#View the BFD session information of Device1.

```
Device1#show bfd session ipv6 2001:1::1 detail
Total ipv6 session number: 1
OurAddr      NeighAddr  LD/RD      State  Holddown  Interface
2001:1::1    2001:1::1  1024/1024  UP     500       vlan2
Type:ipv6 direct Mode:echo
Local Discriminator:66 Remote Discriminator:66
Local State:UP Remote State:UP Up for: 0h:4m:15s Number of times UP:1
Send Interval:100ms Detection time:500ms(100ms*5)
Local Diag:0 Demand mode:0 Poll bit:0
Registered modules:FIB_MGR
```

According to the result, FIB\_MGR has been successfully coordinated with BFD. The session is established normally in the mode of echo.

#When the lines between Device1 and Device3 fail, it can quickly identify the failures and switch to Device2 for communication. The routing table of Device1 shows that the output interface of the destination network 1001:2::/64 has switched to the backup interface vlan3.

```
Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management
L ::1/128 [0/0]
  via ::, 03:03:45, lo0
C 1001:1::/64 [0/0]
  via ::, 02:58:52, vlan4
L 1001:1::1/128 [0/0]
  via ::, 02:58:52, vlan4
O 1001:2::/64 [110/3]
  via fe80::ced8:1fff:fe10:7aae, 00:00:11, vlan3
C 2001:1::/64 [0/0]
  via ::, 02:59:31, vlan2
L 2001:1::1/128 [0/0]
  via ::, 02:59:31, vlan2
C 2001:2::/64 [0/0]
  via ::, 02:58:10, vlan3
L 2001:2::1/128 [0/0]
  via ::, 02:58:10, vlan3
O 2001:3::/64 [110/2]
  via fe80::ced8:1fff:fe10:7aae, 02:53:45, vlan3
```

# 57 IS-IS

---

## 57.1 Overview

IS-IS (Intermediate System to Intermediate System) is an internal gateway protocol (IGP) based on SPF algorithm. The basic design idea and algorithm of IS-IS protocol is almost the same as OSPF. As a routing protocol based on the link layer, IS-IS protocol is not related to or restricted by the network layer (IPv4, IPv6, OSI), so it has good scalability.

IS-IS protocol can support routing of multiple protocol stacks at the same time, including IPv4, IPv6, and OSI. At first, IS-IS protocol was applied in the OSI protocol stack (ISO10589), and then expanded to be used in the routing of IPv4 protocol stack (RFC1195) and IPv6 protocol stack (RFC5308). After expanding, it can support the CSPF calculation of MPLS-TE (RFC3784).

IS-IS protocol is featured by good compatibility (even the extended functions implemented by different devices are inconsistent), large network capacity, simultaneous support of multiple protocol stacks, smooth upgrade, and simpler than OSPF so that it has few problems. Therefore, IS-IS is applicable to large core backbone networks. This section describes how to configure IS-IS dynamic routing protocol on the device for network interconnection.

## 57.2 IS-IS function configuration

Table 57 IS-IS Function Configuration List

Configuration Task	
Configure Basic Functions of IS-IS	Enable IS-IS Protocol
	Configure IS-IS VRF Attributes
Configure Attributes of IS-IS Layer	Configure Attributes of IS-IS Layer
Configure IS-IS Route Generation	Configure IS-IS Default Route
	Configure IS-IS Route Redistribution
Configure IS-IS Route Control	Configure Metric Type of IS-IS
	Configure Metric Value of IS-IS Interface
	Configure IS-IS Administrative Distance
	Configure IS-IS Route Summarization
	Configure the Maximum Number of IS-IS Load Balancing Entries
	Configure IS-IS Inter-area Route Leak
	Configure IS-IS ATT Bit
Configure IS-IS Network Optimization	Configure IS-IS Interface Priority
	Configure Passive IS-IS Interface

Configuration Task	
	Configure Parameters of IS-IS Hello Packets
	Configure Parameters of IS-IS LSP Packets
	Configure Parameters of IS-IS SNP Packets
	Configure IS-IS SPF Calculation Interval
	Configure the Maximum Number of IS-IS Areas
	Configure IS-IS Host Name Mapping
	Add IS-IS Interface to Mesh Group
	Configure IS-IS Network Authentication
Configure IS-IS Network Authentication	Configure IS-IS Neighbor Authentication
	Configure IS-IS Route Authentication
Configure Coordination of IS-IS with BFD	Configure Coordination of IS-IS with BFD
Configure IS-IS GR	Configure IS-IS GR

## 57.2.1 Configure Basic Functions of IS-IS

### Configuration Condition

Before using the IS-IS protocol, ensure that:

- The link layer protocol has been configured to ensure normal communication at the link layer.
- Configure address of interface at network layer so that neighbor network nodes are reachable at the network layer.

### Enable IS-IS Protocol

Multiple IS-IS processes can run in the system, and each of them is distinguished by process name.

Table 57 Enabling IS-IS Protocol

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Create IS-IS process and enter IS-IS configuration mode	<b>router</b> isis [ <i>area-tag</i> ]	Mandatory By default, there is no IS-IS process running in the system, and <i>area-tag</i> is a process name.
Configure network entity title for IS-IS	<b>net</b> <i>entry-title</i>	Mandatory By default, IS-IS doesn't have network entity title.
Return to the global configuration mode	<b>exit</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Enable IS-IS protocol for the interface	<b>ip router</b> isis [ <i>area-tag</i> ]	Mandatory By default, IS-IS protocol is disabled on the interface.

### Note

- IS-IS cannot be run if there is no network entity title.

### Configure IS-IS VRF Attributes

Table 1 Configuring IS-IS VRF Attributes

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the IS-IS configuration mode	<b>router</b> isis [ <i>area-tag</i> ]	-
Configure IS-IS VRF attributes	<b>vrf</b> <i>vrf-name</i>	Optional By default, the IS-IS process is within the global VRF.

## 57.2.2 Configure Attributes of IS-IS Layer

### Configuration Condition

Before configuring attributes of IS-IS layer, ensure that:

- Interface IP addresses have been configured so that neighbor nodes are reachable at the network layer.
- Enable IS-IS Protocol.

### Configure Attributes of IS-IS Layer

Attributes of IS-IS layer have two types, i.e. global layer attributes and interface layer attributes. Global layer attributes are the categories of IS-IS intermediate system. They are divided into the following three categories:

- Level-1 intermediate system: It has Level-1 link status database only, and can advertise and learn routes in Level-1 area only;
- Level-2 intermediate system: It has Level-2 link status database only, and can advertise and learn routes in Level-2 area only;
- Level-1-2 intermediate system: It has both Level-1 and Level-2 link status databases, and can advertise and learn both Level-1 and Level-2 routes. It is an interconnecting device in Level-1 and Level-2 area.

The IS-IS interface layer attributes also have three types:

- Level-1 interface: It can send and receive Level-1 packets of IS-IS protocol only, and can establish Level-1 neighbors only;
- Level-2 interface: It can send and receive Level-2 packets of IS-IS protocol only, and can establish Level-2 neighbors only;
- Level-1-2 interface: It can send and receive both Level-1 and Level-2 packets of IS-IS protocol, and can establish both Level-1 and Level-2 neighbors.

IS-IS interface layer attributes rely on IS-IS global layer attributes. Level-1 intermediate system can own Level-1 interface only, Level-2 intermediate system can own Level-2 interface only, and Level-1-2 intermediate system can own all interfaces at the same time.

Table 2 Configuring IS-IS Global Layer Attributes

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the IS-IS configuration mode	<b>router isis</b> <i>[area-tag]</i>	-

Step	Command	Description
Configure IS-IS global layer attributes	<b>is-type { level-1   level-1-2   level-2-only }</b>	Optional By default, the IS-IS global layer attribute is Level-1-2.

Table 3 Configuring IS-IS Interface Layer Attributes

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface <i>interface-name</i></b>	-
Configure interface layer attributes	<b>isis circuit-type [ level-1   level-1-2   level-2 ]</b>	Optional By default, when the interface layer attributes are not specified, they are consistent with global layer attributes.

### 57.2.3 Configure IS-IS Route Generation

#### Configuration Condition

Before configuring IS-IS route generation, ensure that:

- Interface IP addresses have been configured so that neighbor nodes are reachable at the network layer.
- Enable IS-IS Protocol.

#### Configure IS-IS Default Route

The Level-2 area of IS-IS protocol cannot generate a default route during operation. You may add the default route (with the destination address 0.0.0.0/0) information in the Level-2 LSP and send it. After this information is received by the areas of the same level of other intermediate systems, they will add a default route to the routing table.

Table 4 Configuring IS-IS Default Route

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the IS-IS configuration mode	<b>router isis [ area-tag ]</b>	-
Enter the IS-IS IPv4 address family configuration mode	<b>address-family ipv4 unicast</b>	-
Configure IS-IS to distribute default route	<b>default-information originate</b>	Mandatory By default, the default route is not advertised.

### Configure IS-IS Route Redistribution

The routing information of other routing protocols can be imported into the IS-IS protocol through route redistribution so that the AS where IS-IS protocol is running is interconnected with the AS or routing domain where other routing protocol is running. When importing external route, you may specify the route importing policy and the layer attributes after the route is imported.

Table 57 Configuring IS-IS Route Redistribution

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the IS-IS configuration mode	<b>router isis [ area-tag ]</b>	-
Enter the IS-IS IPv4 address family configuration mode	<b>address-family ipv4 unicast</b>	-
Configure IS-IS Route Redistribution	<b>redistribute protocol [ protocol-id ] [ level-1 / level-1-2 / level-2 / metric metric-value / metric-type { external   internal } / route-map route-map-name / match route-sub-type ]</b>	Mandatory By default, the information of other routing protocol is not redistributed.

## 57.2.4 Configure IS-IS Route Control

### Configuration Condition

Before configuring IS-IS routing features, ensure that:

- Interface IP addresses have been configured so that neighbor nodes are reachable at the network layer.
- Enable IS-IS Protocol.

### Configure Metric Type of IS-IS

The initial IS-IS only has a narrow metric. When narrow metric is used, the maximum metric value of the interface is 63. With the gradual expansion of the network size, narrow metric is far from meeting the demand. Therefore, the metric type is expanded later to include wide metric which can reach 16777214. Devices using different metric types cannot advertise and learn routing information from each other. In order to achieve the transition between the two metric types, a configuration method for transiting metric type is provided.

Wide metric is recommended.

Table 5 Configuring IS-IS Metric Type

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the IS-IS configuration mode	<b>router isis [area-tag]</b>	-
Configure the metric type of interface	<b>metric-style {narrow   narrow transition   transition   wide   wide transition} [level-1   level-1-2   level-2]</b>	Optional By default, narrow metric is used.

### Configure Metric Value of IS-IS Interface

After IS-IS protocol is enabled on the interface, the metric of IS-IS route is the global metric value, which can be separately specified for each interface through command.

Table 6 Configuring Metric Value of Interface

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the IS-IS configuration mode	<b>router isis</b> [ <i>area-tag</i> ]	-
Configure IS-IS global metric value	<b>metric</b> <i>metric-value</i> [ <b>level-1</b>   <b>level-2</b> ]	Optional By default, the global metric value is 10.
Return to the global configuration mode	<b>exit</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure the metric value of interface	isis <b>ipv4 metric</b> { <i>metric-value</i>   <b>maximum</b> } [ <b>level-1</b>   <b>level-2</b> ]	Optional By default, the global metric value is used.

### Configure IS-IS Administrative Distance

The system selects routes according to the administrative distance. The smaller the administrative distance, the higher the route priority.

Table 7 Configuring IS-IS Administrative Distance

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the IS-IS configuration mode	<b>router isis</b> [ <i>area-tag</i> ]	-
Enter the IS-IS IPv4 address family configuration mode	<b>address-family ipv4 unicast</b>	-
Configure the administrative distance of IS-IS route	<b>distance</b> <i>distance-value</i>	Optional By default, the administrative distance is 115.

### Configure IS-IS Route Summarization

Route summarization can summarize multiple pieces of routing information into one piece of routing information. After IS-IS is configured with route summarization, it can effectively reduce the number of subnet information reachable through advertisement, and reduce the size of the link status database and routing table, so as to effectively save memory and CPU resources. This configuration is generally used on Level-1-2 edge devices to reduce the routing information advertised between layers.

Table 8 Configuring IS-IS Route Summarization

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the IS-IS configuration mode	<b>router isis [area-tag]</b>	-
Enter the IPv4 address family configuration mode	<b>address-family ipv4 unicast</b>	-
Configure IS-IS Route Summarization	<b>summary-prefix prefix-value [ metric metric-value / route-type {internal   external} / metric-type {internal   external} / tag tag-value / not-advertise / level-1 / level-2 / level-1-2 ]</b>	Mandatory By default, route summarization is disabled.

### Configure the Maximum Number of IS-IS Load Balancing Entries

There may be multiple paths with the same cost that lead to the same destination address. These equal-cost paths can improve link utilization rate. Users can control the maximum number of IS-IS equal-cost routes.

Table 9 Configuring Maximum Number of IS-IS Load Balancing Entries

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the IS-IS configuration mode	<b>router isis [area-tag]</b>	-
Enter the IPv4 address family configuration mode	<b>address-family ipv4 unicast</b>	-

Step	Command	Description
Configure the Maximum Number of IS-IS Load Balancing Entries	<b>maximum-paths</b> <i>max-number</i>	Optional By default, the maximum number of load balancing entries is 4.

### Configure IS-IS Inter-area Route Leak

By default, IS-IS only leaks Level-1 routes to Level-2, and Level-1 areas cannot know the routes in Level-2 area. You can import Level-2 routes to Level-1 by configuring inter-layer route leak. When configuring inter-layer route leak, you can specify a routing policy to only leak the route which match the conditions.

Table 10 Configuring IS-IS Inter-layer Route Leak

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the IS-IS configuration mode	<b>router isis</b> [ <i>area-tag</i> ]	-
Enter the IS-IS IPv4 address family configuration mode	<b>address-family ipv4 unicast</b>	-
Configure IS-IS Inter-area Route Leak	<b>propagate</b> { <b>level-1 into level-2</b>   <b>level-2 into level-1</b> } [ <b>distribute-list</b> <i>access-list-name</i>   <b>route-map</b> <i>route-map-name</i> ]	Mandatory By default, Level-1 leaks routes to Level-2.

### Configure IS-IS ATT Bit

In Level-1-2 devices, ATT bit is used to advertise other nodes whether this node has connections with other areas. If yes, ATT bit will be set as 1 automatically, and other nodes will produce a default route towards this node. This will increase the business burden of this node. To change this situation, you can set ATT bit as 0.

Table 11 Configuring IS-IS ATT Bit

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Enter the IS-IS configuration mode	<b>router</b> isis [ <i>area-tag</i> ]	-
Enter the IS-IS IPv4 address family configuration mode	<b>address-family ipv4 unicast</b>	-
Configure IS-IS ATT Bit	<b>set-attached-bit { on   off }</b>	Mandatory By default, ATT bit is set based on whether a node has connected with other areas.

## 57.2.5 Configure IS-IS Network Optimization

### Configuration Condition

Before configuring IS-IS adjustment and optimization, ensure that:

- Interface IP addresses have been configured so that neighbor nodes are reachable at the network layer.
- Enable IS-IS Protocol.

### Configure IS-IS Interface Priority

On the broadcast link, IS-IS needs to elect a node as DIS. DIS nodes send CSNP packets on a regular basis to synchronize the link status database across the network. The Level-1 and Level-2 DIS nodes are separately elected. Those with the highest interface priority are elected as DIS nodes. When the priority is the same, those with a large MAC address as DIS nodes.

Table 12 Configuring IS-IS Interface Priority

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure IS-IS Interface Priority	isis <b>priority</b> <i>priority-value</i> [ <b>level-1</b>   <b>level-2</b> ]	Optional By default, the interface priority is 64.

## Configure Passive IS-IS Interface

Passive interface means the interface where no IS-IS protocol packets will be sent or received, though its direct network routing information is distributed; configuring passive IS-IS interface can save both bandwidth and the processing time of CPU; on this basis, IS-IS can also be specified to distribute direct network routing information of passive interface rather than of non-passive interface.

Table 13 Configuring Passive IS-IS Interface

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the IS-IS configuration mode	<b>router isis</b> [ <i>area-tag</i> ]	-
Configure Passive IS-IS Interface	<b>passive-interface</b> <i>interface-name</i>	Mandatory By default, there is no passive interface in IS-IS.
Configure IS-IS to distribute the routing information of passive interface only	<b>advertise-passive-only</b>	Optional By default, all the information of direct network routes that have enabled IS-IS protocol interface is distributed.

## Configure Parameters of IS-IS Hello Packets

1. Configure Hello packet sending interval

After the IS-IS protocol interface is enabled, Hello packets will be periodically sent to maintain neighbor relations. The smaller the Hello packet sending interval, the larger the network convergence and the bandwidth occupied.

Table 14 Configuring Hello Packet Sending Interval

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-

Step	Command	Description
Configure Hello packet sending interval for the interface	isis <b>hello-interval</b> { <i>interval</i>   <b>minimal</b> } [ <b>level-1</b>   <b>level-2</b> ]	Optional By default, the Hello packet sending interval is 10 seconds.

## 2. Configure the number of invalid Hello packets

S-IS calculates the time of maintaining neighbor relations according to the number of invalid Hello packets, and advertise such time to neighbor devices. If the neighbor device fails to receive the Hello packets from this device during this time, it is believed the neighbor relation has become invalid, and routing calculation will be done anew.

Table 15 Configuring Number of Invalid Hello Packets

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure the number of invalid Hello packets on the interface	isis <b>hello-multiplier</b> <i>multiplier</i> [ <b>level-1</b>   <b>level-2</b> ]	Optional By default, the number of invalid Hello packets is 3.

## 3. Cancel Hello packet filling

If the MTU values of the interfaces at both ends of the link are inconsistent, large packets will not be able to pass through. To avoid this situation, IS-IS fills Hello packets to the MTU value of interface so that neighbor relation cannot be established. However, this method causes a waste of bandwidth. In actual applications, you can cancel Hello packet filling to send small Hello packets.

Table 16 Configuring Function of Cancelling Hello Packet Filling

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-

Step	Command	Description
Cancel Hello packet filling	<b>no isis hello padding</b>	Mandatory By default, the Hello packet filling function is enabled.

### Configure Parameters of IS-IS LSP Packets

1. Configure the maximum Time-To-Live of LSP packets

Each LSP packet has a maximum Time-To-Live. After decreasing to zero, the Time-To-Live of LSP packets will be deleted from the link status database. The maximum Time-To-Live of LSP packets shall be greater than their refresh interval.

Table 17 Configuring Parameters of IS-IS LSP Packet

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the IS-IS configuration mode	<b>router isis [area-tag]</b>	-
Configure the maximum Time-To-Live of LSP packets	<b>max-lsp-lifetime</b> <i>life-time</i>	Optional By default, the maximum Time-To-Live of LSP packets is 1200 seconds.

2. Configure LSP packet refresh interval

The IS-IS protocol advertises and learns routes by interacting with their respective LSP packets. The node stores the LSP packets received in its own link state database. Each LSP packet has a maximum Time-To-Live, so all nodes need to update their LSP packets on a regular basis to prevent the maximum Time-To-Live of LSP packets from reducing to zero, and to keep the LSP packets in the entire area synchronized. Reducing the periodic LSP packet sending interval can accelerate network convergence, though it will occupy a larger bandwidth.

Table 18 Configuring LSP Packet Refresh Interval

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Enter the IS-IS configuration mode	<b>router</b> isis [ <i>area-tag</i> ]	-
Configure LSP packet refresh interval	<b>lsp-refresh-interval</b> <i>refresh-interval</i>	Optional By default, the period sending interval is 900 seconds.

### 3. Configure LSP packet generation interval

In addition to periodic update, change of interface and network status can trigger generation of new LSP packets. To avoid frequent generation of LSP packets to occupy a large amount of CPU resources, users can configure the minimum LSP packet generation interval.

Table 19 Configuring LSP Packet Generation Interval

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the IS-IS configuration mode	<b>router</b> isis [ <i>area-tag</i> ]	-
Configure LSP packet generation interval	<b>lsp-gen-interval</b> [ <b>level-1</b>   <b>level-2</b> ] <i>max-interval</i> [ <i>initial-interval</i> [ <i>secondary-interval</i> ] ]	Optional By default, the upper limit and lower limit of LSP packet generation interval are 10 seconds and 50 milliseconds.

### 4. Configure LSP packet sending interval

Whenever LSP packets are generated, they are sent on the interface. To avoid frequent generation of LSP packets to occupy massive interface bandwidth, you can configure the minimum LSP packet sending interval for each interface.

Table 20 Configuring LSP Packet Sending Interval

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure LSP packet sending interval	isis <b>lsp-interval</b> <i>min-interval</i>	Optional By default, the LSP packet sending interval is 33 milliseconds.

#### 5. Configure LSP packet retransmission time

On the point-to-point link, IS-IS needs to send a PSNP confirmation message from the peer port after sending LSP packet. If the confirmation message from the peer port fails to be received, the LSP packet will be resent. The time of waiting for confirmation, i.e. the LSP packet retransmission time, can be configured by users to prevent LSP packets from being retransmitted because the confirmation is not received when there is a long time delay.

Table 21 Configuring LSP Packet Retransmission Time

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure LSP packet retransmission time	isis <b>retransmit-interval</b> <i>interval [ level-1   level-2 ]</i>	Optional By default, the retransmission time is 5 seconds.

#### 6. Configure LSP MTU value

IS-IS protocol packets cannot be automatically fragmented. To ensure normal diffusion of LSP packets, the maximum length of LSP packets in a routing domain shall not exceed the minimum MTU value of the IS-IS interface of all devices; when the MTU values of the device interfaces in the routing domain are inconsistent, uniform setting of the maximum LSP packet length is recommended.

Table 22 Configuring LSP MTU Value

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the IS-IS configuration mode	<b>router</b> isis [ <i>area-tag</i> ]	-
Configure MTU value of LSP packet	<b>lsp-mtu</b> <i>mtu-size</i> [ <b>level-1</b>   <b>level-2</b> ]	Optional By default, the MTU value of LSP packet is 1492 bytes.

### Configure Parameters of IS-IS SNP Packets

#### 1. Configure CSNP packet sending interval

The broadcast link election node needs to periodically send CSNP packets to synchronize the link status database of the entire network. The periodic sending interval of CSNP packets can be adjusted based on the actual situation.

Table 23 Configuring CSNP Packet Sending Interval

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure CSNP packet sending interval	isis <b>csnp-interval</b> <i>interval</i> [ <b>level-1</b>   <b>level-2</b> ]	Optional By default, the periodic CSNP packet sending interval is 10 seconds.

#### 2. Configure PSNP packet sending interval

On the broadcast link, PSNP packets are used to synchronize the link status database of the entire network; on the point-to-point link, PSNP packets are used to confirm the received LSP packets. In order to prevent a large number of PSNP packets from being sent on the interface, a minimum sending time interval is set for PSNP packets. Users can dynamically modify this interval. A very large PSNP packet sending interval is not recommended. For broadcast links, it will affect the synchronization of the link status database of the entire network. For point-to-point links, it will cause the retransmission of LSP packets due to late receipt of confirmation.

Table 24 Configuring PSNP Packet Sending Interval

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure PSNP packet sending interval	<b>isis psnp-interval</b> <i>min-interval</i> [ <b>level-1</b>   <b>level-2</b> ]	Optional By default, the PSNP packet sending interval is 2 seconds.

### Configure IS-IS SPF Calculation Interval

The change of IS-IS link status database will trigger SPF routing calculation. Frequent SPF calculation consumes a great many CUP resources. Users may configure the SPF calculation interval.

Table 25 Configuring IS-IS SPF Calculation Interval

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the IS-IS configuration mode	<b>router isis</b> [ <i>area-tag</i> ]	-
Enter the IS-IS IPv4 address family configuration mode	<b>address-family ipv4 unicast</b>	-
Configure IS-IS SPF calculation interval	<b>spf-interval</b> [ <b>level-1</b>   <b>level-2</b> ] <i>maximum-interval</i> [ <i>min-initial-delay</i> [ <i>min-second-delay</i> ] ]	Optional

### Configure the Maximum Number of IS-IS Areas

An IS-IS process can be configured with multiple area addresses that are mainly used for the smooth transition of merging multiple Level-1 areas into one Level-1 area, or dividing a Level-1 area into multiple Level-1 areas.

Table 26 Configuring Maximum Number of Areas for IS-IS

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the IS-IS configuration mode	<b>router isis</b> [ <i>area-tag</i> ]	-
Configure the Maximum Number of IS-IS Areas	<b>max-area-addresses</b> <i>max-number</i>	Optional By default, the maximum number of area addresses is 3.

### Note

- This requires consistent configuration in the entire IS-IS Level-1 routing domain. Otherwise, Level-1 neighbors cannot be normally established. This is not the case for Level-2 neighbors.

### Configure IS-IS Host Name Mapping

IS-IS can uniquely identify an intermediate system through system ID. The fixed length of the system ID is 6 bytes. When viewing system information (e.g. neighbor relation, and link status database), users cannot link the system ID with host name; IS-IS supports the mapping of system ID and host name for intuitive and convenient viewing of system information by users. There are two ways to configure IS-IS host name mapping:

1. Configure IS-IS static host name mapping

IS-IS static host name mapping means the mapping that users manually establish system ID and host name for remote devices.

Table 27 Configuring IS-IS Static Host Name Mapping

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the IS-IS configuration mode	<b>router isis</b> [ <i>area-tag</i> ]	-
Configure IS-IS static host name mapping	<b>hostname static</b> <i>system-id</i> <i>host-name</i>	Mandatory

2. Configure IS-IS dynamic host name mapping

Static host name mapping requires users to configure system ID and host name mapping of other devices for each device in the network, which is a heavy workload; for dynamic host name mapping, other devices in the network can learn the host name of the device after configuring host name for each device and enabling the host name advertisement function.

Table 28 Configuring IS-IS Dynamic Host Name Mapping

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the IS-IS configuration mode	<b>router isis</b> [ <i>area-tag</i> ]	-
Configure IS-IS dynamic host name mapping	<b>hostname dynamic</b> { <i>host-name</i>   <b>area-tag</b>   <b>recv-only</b>   <b>system-name</b> }	Mandatory By default, only the host name advertised by other devices is learned.

#### Add IS-IS Interface to Mesh Group

Without being added into the Mesh group, the IS-IS interface will send the LSP packet received from an interface via all the other IS-IS interfaces. This causes a huge waste of bandwidth in the fully meshed network. You may add several IS-IS interfaces into the same Mesh group. After receiving the LSP packet, the interfaces only send this packet to the interfaces in other Mesh group.

Table 29 Adding IS-IS Interface into Mesh Group

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Add IS-IS Interface to Mesh Group	isis <b>mesh-group</b> { <i>group-number</i>   <b>blocked</b> }	Mandatory By default, it is not added into any Mesh group.

#### Note

- **isis mesh-group blocked** sets the interface as a blocking interface. The blocking interface

---

will not actively send LSP packets. It does so only when LSP request is received.

---

## 57.2.6 Configure IS-IS Network Authentication

### Configuration Condition

Before configuring IS-IS network authentication, ensure that:

- Interface IP addresses have been configured so that neighbor nodes are reachable at the network layer.
- Enable IS-IS Protocol.

### Configure IS-IS Neighbor Authentication

After configuring IS-IS to enable neighbor relation authentication, an authentication message will be added into the Hello packet sent, and the Hello packet received will be authenticated. If the authentication fails, a neighbor relation cannot be formed. This will prevent the establishment of neighbor relation with the device which cannot be trusted.

Table 30 Configuring IS-IS Neighbor Authentication

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure Hello packet authentication mode	<b>isis authentication mode</b> { <b>md5</b>   <b>sm3</b>   <b>text</b> } [ <b>level-1</b>   <b>level-2</b> ]	Mandatory  By default, the authentication function is disabled.
Configure the authentication password of Hello packet	<b>isis authentication key</b> { <b>0</b>   <b>7</b> } <i>password</i> [ <b>level-1</b>   <b>level-2</b> ]	Either-or  By default, there is no authentication password; authentication password can be configured with a coding strand. For the configuration of coding strand, see the coding strand configuration section in the User Manual.
	<b>isis authentication key-chain</b> <i>key-chain-name</i> [ <b>level-1</b>   <b>level-2</b> ]	

### Configure IS-IS Route Authentication

After configuring IS-IS routing information authentication, an authentication message will be added into the LSP and SNP packet, and the LSP and SNP packet received will be authenticated. If the authentication fails, the packet will be directly discarded. This will prevent the routing information which cannot be trusted from diffusing into the IS-IS network.

Table 31 Configuring IS-IS Route Authentication

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the IS-IS configuration mode	<b>router isis</b> [ <i>area-tag</i> ]	-
Configure the authentication mode of routing information packet	<b>authentication mode</b> { <b>md5</b>   <b>sm3</b>   <b>text</b> } [ <b>level-1</b>   <b>level-2</b> ]	Mandatory  By default, the authentication function is disabled.
Configure the authentication password of routing information packet	<b>authentication key</b> { <b>0</b>   <b>7</b> } <i>password</i> [ <b>level-1</b>   <b>level-2</b> ]	Either-or  By default, there is no authentication password; authentication password can be configured with a coding strand. For the configuration of coding strand, see the coding strand configuration section in the User Manual.
	<b>authentication key-chain</b> <i>key-chain-name</i> [ <b>level-1</b>   <b>level-2</b> ]	

### 57.2.7 Configure Coordination of IS-IS with BFD

Configuring the coordination of IS-IS with BFD can quickly detect link failures so as to enable backup link for communication. There are two ways to configure the coordination of IS-IS with BFD: associate BFD for all the interfaces that have enabled IS-IS protocol; specify the interface to associate BFD.

For BFD parameters, see the BFD configuration manual.

#### Configuration Condition

Before configuring the coordination of IS-IS with BFD, ensure that:

- Interface IP addresses have been configured so that neighbor nodes are reachable at the network layer.
- Enable IS-IS Protocol.

## Configure Coordination of IS-IS with BFD

Table 32 Configuring Coordination of IS-IS with BFD

Step	Command
Enter the global configuration mode.	<b>configure terminal</b>
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>
Enable the BFD link detection function on the interface	isis <b>bfd</b>
Return to the global configuration mode	<b>exit</b>
Enter the IS-IS configuration mode	<b>router</b> isis [ <i>area-tag</i> ]
Enable the BFD link detection function on the IS-IS interface	<b>bfd all-interfaces</b>

### 57.2.8 Configure IS-IS FRR

#### Configuration Condition

Before configuring IS-IS FRR, ensure that:

- Interface IP addresses have been configured so that neighbor nodes are reachable at the network layer.
- Enable IS-IS Protocol.

#### Configure IS-IS FRR

In the IS-IS network, as a result of link or device failure, the packets passing the point of failure will be discarded or loops will be produced. The traffic interruption caused thereby will continue until the protocol reconverges after several seconds. In order to reduce the time of traffic interruption, IS-IS FRR can be configured. By applying the routing map, set a backup next hop for the successfully matched route. Once the main link fails, the traffic passing through the failed link will immediately switch to the backup link, achieving the purpose of fast switching.

Table 33 Configuring IS-IS FRR

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Enter the IS-IS configuration mode	<b>router isis</b> [ <i>area-tag</i> ]	-
Enter the IS-IS IPv4 address family configuration mode	<b>address-family ipv4 unicast</b>	-
Configure ISIS to enable the FRR function	<b>fast-reroute route-map</b> <i>route-map-name</i>	Mandatory By default, the IS-IS FRR function is disabled.
Configure IS-IS to enable the dynamic FRR function	<b>fast-reroute loop-free-alternate</b> [route-map <i>route-map-name</i> ]	Mandatory By default, the IS-IS dynamic FRR function is disabled.
Configure IS-IS to enable the pic function	<b>pic</b>	Mandatory After the pic function is enabled, the auto FRR function is enabled. By default, the IS-IS pic function is disabled.

## Note

- The IS-IS FRR function has two types, i.e. static FRR and dynamic FRR.
- Static FRR needs to associate route-map where the next hop interface and address of back-up route are set.
- Currently, dynamic FRR supports point-to-point network only, i.e. all the output interfaces of the device have a network type of point-to-point. After dynamic FRR is configured, the device automatically calculates and sets back-up next hop interface and address. Dynamic FRR can also associate route-map to set back-up next hop interface and address for the route which matches the route-map only.
- The methods of enabling rerouting are mutually exclusive;

### 57.2.9 Configure IS-IS GR

GR (Graceful Restart) is used to keep the routing information in the forwarding layer of this device and neighbor device unchanged during the switch between host and standby devices to ensure the forwarding

process is not affected; after the device is switched for re-running, the two devices synchronize routing information and update forwarding layer in the protocol layer so that the data can keep forwarding during the process of device switch.

There are two types of roles in the GR process:

GR Restarter end: The device for graceful restart of protocol.

GR Helper end: The device which helps with the graceful restart of protocol.

The distributed device can act as GR Restarter and GR Helper, while the centralized device only serves as GR Helper to help the Restarter complete GR.

### Configuration Condition

Before configuring IS-IS GR, ensure that:

- Interface IP addresses have been configured so that neighbor nodes are reachable at the network layer.
- Enable IS-IS Protocol.

### Configure IS-IS GR Restarter

Table 34 Configuring IS-IS GR Restarter

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the IS-IS configuration mode	<b>router isis [ <i>area-tag</i> ]</b>	-
Enable IS-IS to enable the GR function	<b>nsf ietf</b>	Mandatory By default, the GR function is disabled.
Configure advertisement to enter the retransmission times of GR process message	<b>nsf interface-expire <i>resend-cnt</i></b>	Optional By default, the number of retransmission times is 3.
Configure the retransmission waiting time of GR process message	<b>nsf interface-timer <i>wait-time</i></b>	Optional By default, the waiting time is 10 seconds.

### Configure IS-IS GR Helper

GR Helper can help the Restarter end complete GR. By default, the device enables this function. Users can close this function via command.

Table 35 Configuring IS-IS GR Helper

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the IS-IS configuration mode	<b>router isis [ area-tag ]</b>	-
Configure IS-IS GR Helper to disable the capability of Helper	<b>nsf ietf helper-disable</b>	Mandatory Configure IS-IS GR Helper to disable the capability of Helper

## 57.2.10IS-IS monitoring and maintaining

Table 36 IS-IS Monitoring and Maintaining

Command	Description
<b>clear isis [ instance -null   area-tag ] statistics [ interface_name ]</b>	Clear the statistical information of IS-IS protocol operation
<b>clear isis [ instance -null   area-tag ] process</b>	Restart IS-IS protocol process
<b>show isis [ instance -null   area-tag ]</b>	Show the information of IS-IS process
<b>show isis instance { -null   area-tag } ipv4 bfd-sessions</b>	Show the BFD session information of IS-IS process
<b>show isis [ instance -null   area-tag ] database [ lsp_id ] [ detail ] [ l1 / l2 ] [ level-1 / level-2 ] [ self ] [ verbose ]</b>	Show the IS-IS link status database information
<b>show isis interface [ interface-name ] [ detail ]</b>	Show the information of running IS-IS protocol interface
<b>show isis [ instance -null   area-tag ] ipv4 reach-info</b>	Show the IPV4 subnet reachable information of IS-IS

Command	Description
<b>show isis [ instance –null   area-tag ] ipv4 route</b>	Show the IPV4 routing information of IS-IS
<b>show isis [ instance –null   area-tag ] ipv4 topology</b>	Show the IPV4 topological information of IS-IS
<b>show isis [ instance – null   area-tag ] is-reach-info [ level-1   level-2 ]</b>	Show the information about neighboring nodes of IS-IS
<b>show isis [instance –null   area-tag] mesh-groups</b>	Show the mesh group of IS-IS
<b>show isis [ instance –null   area-tag ] neighbors [ interface-name ] [ detail ]</b>	Show the information of IS-IS neighbors
<b>show isis [ instance –null   area-tag ] statistics [ interface-name ]</b>	Show the statistical information of IS-IS protocol operation
<b>show isis router</b>	Show the host name information of IS-IS

## 57.3 Typical configuration example of IS-IS

### 57.3.1 Configure Basic Functions of IS-IS

#### Network Requirements

- Enable network interconnection between devices by configuring IS-IS protocol.
- Device1 is a Level-1 router; Device2 is a Level-1-2 router; Device1 and Device2 are in the same area; the area number is 10. Device3 is a Level-2 router, and the area number is 20. Device2 connects the two areas.

#### Network Topology

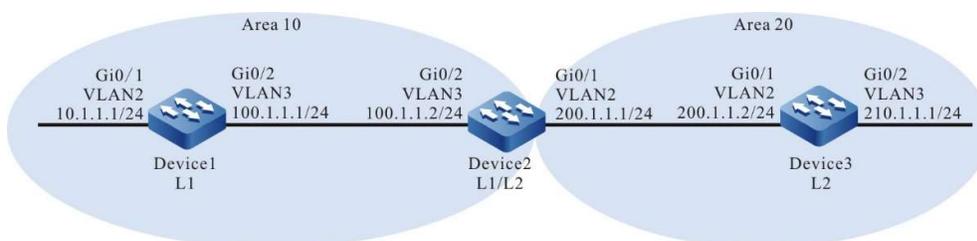


Figure 57 Network Topology for Basic Functions of IS-IS

#### Configuration Steps

Step 1: Configure IP addresses for the ports. (Omitted)

Step 2: Configure IS-IS and enable the this process on the interface.

#On Device1, configure IS-IS process 100, area number 10 and type Level-1, and enable this process on the interface.

```
Device1#configure terminal
Device1(config)#router isis 100
Device1(config-isis)#net 10.0000.0000.0001.00
Device1(config-isis)#is-type level-1
Device1(config-isis)#metric-style wide
Device1(config-isis)#exit
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ip router isis 100
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan3
Device1(config-if-vlan3)#ip router isis 100
Device1(config-if-vlan3)#exit
```

#On Device2, configure IS-IS process 100, area number 10 and type Level-1-2, and enable this process on the interface.

```
Device2#configure terminal
Device2(config)#router isis 100
Device2(config-isis)#net 10.0000.0000.0002.00
Device2(config-isis)#metric-style wide
Device2(config-isis)#exit
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ip router isis 100
Device2(config-if-vlan2)#exit
Device2(config)#interface vlan3
Device2(config-if-vlan3)#ip router isis 100
Device2(config-if-vlan3)#exit
```

#On Device3, configure IS-IS process 100, area number 20 and type Level-2, and enable this process on the interface.

```
Device3#configure terminal
Device3(config)#router isis 100
Device3(config-isis)#net 20.0000.0000.0003.00
Device3(config-isis)#is-type level-2
Device3(config-isis)#metric-style wide
Device3(config-isis)#exit
Device3(config)#interface vlan2
Device3(config-if-vlan2)#ip router isis 100
Device3(config-if-vlan2)#exit
Device3(config)#interface vlan3
Device3(config-if-vlan3)#ip router isis 100
Device3(config-if-vlan3)#exit
```

Step 3: Check the result.

#View the information of IS-IS neighbors on Device1.

```
Device1#show isis neighbors
IS-IS Instance 100 Neighbors (Counter 1):
Type System ID Interface State Holdtime Level IETF-NSF Priority Circuit ID
L1-LAN 0000.0000.0002 vlan3 Up 29 sec L1 capable 64 0000.0000.0001.01
```

#View the information of IS-IS neighbors on Device2.

```

Device2#show isis neighbors
IS-IS Instance 100 Neighbors (Counter 2):
Type System ID Interface State Holdtime Level IETF-NSF Priority Circuit ID
L2-LAN 0000.0000.0003 vlan2 Up 9 sec L2 capable 64 0000.0000.0003.01
L1-LAN 0000.0000.0001 vlan3 Up 8 sec L1 capable 64 0000.0000.0001.01

```

Device2 establishes IS-IS neighbors with Device1 and Device3.

#View the information of IS-IS neighbors on Device 3.

```

Device3#show isis neighbors
IS-IS Instance 100 Neighbors (Counter 1):
Type System ID Interface State Holdtime Level IETF-NSF Priority Circuit ID
L2-LAN 0000.0000.0002 vlan3 Up 22 sec L2 capable 64 0000.0000.0003.01

```

#View the routing information of Device1.

```

Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

i 0.0.0.0/0 [115/10] via 100.1.1.2, 17:44:09, vlan3
C 10.1.1.0/24 is directly connected, 16:56:18, vlan2
C 100.1.1.0/24 is directly connected, 18:37:57, vlan3
C 127.0.0.0/8 is directly connected, 284:02:13, lo0
i 200.1.1.0/24 [115/20] via 100.1.1.2, 17:44:09, vlan3

```

```

Device1#show isis ipv4 route
IS-IS Instance 100, VRF Kernel, IPv4 routes table (Counter 4):
L1 0.0.0.0/0, flags none, metric 10, from learned, installed
   via 100.1.1.2, vlan3, neighbor 0000.0000.0002
L1 10.1.1.0/24, flags none, metric 10, from network connected
   via 0.0.0.0, vlan2
L1 100.1.1.0/24, flags none, metric 10, from network connected
   via 0.0.0.0, vlan3
L1 200.1.1.0/24, flags none, metric 20, from learned, installed
   via 100.1.1.2, vlan3, neighbor 0000.0000.0002

```

There is a default route in the routing table of Device1. The next hop is Device2.

#View the routing information of Device2.

```

Device2#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

i 10.1.1.0/24 [115/20] via 100.1.1.1, 16:58:26, vlan3
C 100.1.1.0/24 is directly connected, 18:39:58, vlan3
C 127.0.0.0/8 is directly connected, 20:16:34, lo0
C 200.1.1.0/24 is directly connected, 18:39:37, vlan2
i 210.1.1.0/24 [115/20] via 200.1.1.2, 16:57:56, vlan2

```

```

Device2#show isis ipv4 route
IS-IS Instance 100, VRF Kernel, IPv4 routes table (Counter 4):
L1 10.1.1.0/24, flags none, metric 20, from learned, installed
   via 100.1.1.1, vlan3, neighbor 0000.0000.0001
L1 100.1.1.0/24, flags none, metric 10, from network connected
   via 0.0.0.0, vlan3
L1 200.1.1.0/24, flags none, metric 10, from network connected
   via 0.0.0.0, vlan2
L2 210.1.1.0/24, flags none, metric 20, from learned, installed
   via 200.1.1.2, vlan2, neighbor 0000.0000.0003
Device2 includes Level-1 and Level-2 routes.

```

#View the routing information of Device3.

```
Device3#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
i 10.1.1.0/24 [115/30] via 200.1.1.1, 16:59:29, vlan2
i 100.1.1.0/24 [115/20] via 200.1.1.1, 17:47:29, vlan2
C 127.0.0.0/8 is directly connected, 945:29:12, lo0
C 200.1.1.0/24 is directly connected, 18:40:27, vlan2
C 210.1.1.0/24 is directly connected, 16:59:04, vlan3
```

```
Device3#show isis ipv4 route
IS-IS Instance 100, VRF Kernel, IPv4 routes table (Counter 4):
L2 10.1.1.0/24, flags none, metric 30, from learned, installed
   via 200.1.1.1, vlan2, neighbor 0000.0000.0002
L2 100.1.1.0/24, flags none, metric 20, from learned, installed
   via 200.1.1.1, vlan2, neighbor 0000.0000.0002
L2 200.1.1.0/24, flags none, metric 10, from network connected
   via 0.0.0.0, vlan2
L2 210.1.1.0/24, flags none, metric 10, from network connected
   via 0.0.0.0, vlan3
```

Device3 learns Level-1 route. By default, Level-1 leaks to Level-2.

---

## Note

- The metric type is narrow metric by default. Wide metric is recommended.
  - The IS-IS entity attribute is Level-1-2 by default.
- 

## 57.3.2 Configure the DIS election of IS-IS

### Network Requirements

- Specify the device as DIS by modifying priority.
- Both Device1 and Device2 are Level-1-2 devices; Device3 is a Level-1 device; Device4 is a Level-2 device. Device1, Device2, Device3, and Device4 are in the same broadcast network and area, with the area number being 10.

### Network Topology

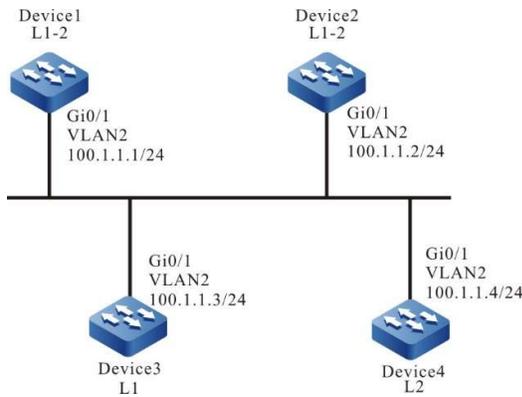


Figure 1 Network Topology for Configuring DIS Election of IS-IS

### Configuration Steps

Step 1: Configure IP addresses for the ports. (Omitted)

Step 2: Configure IS-IS and enable the this process on the interface.

#On Device1, configure IS-IS process 100, area number 10 and type Level-1-2, and enable this process on the interface.

```

Device1#configure terminal
Device1(config)#router isis 100
Device1(config-isis)#net 10.0000.0000.0001.00
Device1(config-isis)#metric-style wide
Device1(config-isis)#exit
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ip router isis 100
Device1(config-if-vlan2)#exit
  
```

#On Device2, configure IS-IS process 100, area number 10 and type Level-1-2, and enable this process on the interface.

```

Device2#configure terminal
Device2(config)#router isis 100
Device2(config-isis)#net 10.0000.0000.0002.00
Device2(config-isis)#metric-style wide
Device2(config-isis)#exit
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ip router isis 100
Device2(config-if-vlan2)#exit
  
```

#On Device3, configure IS-IS process 100, area number 10 and type Level-1, and enable this process on the interface.

```

Device3#configure terminal
Device3(config)#router isis 100
Device3(config-isis)#net 10.0000.0000.0003.00
Device3(config-isis)#is-type level-1
Device3(config-isis)#metric-style wide
Device3(config-isis)#exit
Device3(config)#interface vlan2
Device3(config-if-vlan2)#ip router isis 100
Device3(config-if-vlan2)#exit
  
```

#On Device4, configure IS-IS process 100, area number 20 and type Level-2, and enable this process on the interface.

```

Device4#configure terminal
Device4(config)#router isis 100
Device4(config-isis)#net 20.0000.0000.0004.00
Device4(config-isis)#is-type level-2
Device4(config-isis)#metric-style wide
Device4(config-isis)#exit
Device4(config)#interface vlan2
Device4(config-if-vlan2)#ip router isis 100
Device4(config-if-vlan2)#exit

```

#View the information of IS-IS neighbors on Device1.

```

Device1#show isis neighbors
IS-IS Instance 100 Neighbors (Counter 4):
Type System ID Interface State Holdtime Level IETF-NSF Priority Circuit ID
L1-LAN 0000.0000.0002 vlan2 Up 23 sec L1 capable 64 0000.0000.0003.01
L2-LAN 0000.0000.0002 vlan2 Up 23 sec L2 capable 64 0000.0000.0004.01
L1-LAN 0000.0000.0003 vlan2 Up 8 sec L1 capable 64 0000.0000.0003.01
L2-LAN 0000.0000.0004 vlan2 Up 8 sec L2 capable 64 0000.0000.0004.01

```

The pseudo node of Level-1 is 0000.0000.0003.01, and Device3 is the DIS of Level-1. The pseudo node of Level-2 is 0000.0000.0004.01, and Device4 is the DIS of Level-2.

#Use the command **show isis interface** to view the MAC address of the interface. In the default priority, DIS is selected according to the principle that the larger the MAC address of the physical interface, the higher the priority.

Step 3: Modify interface priority.

#Modify the priority of Device1 interface.

```

Device1(config)#interface vlan2
Device1(config-if-vlan2)#isis priority 100
Device1(config-if-vlan2)#exit

```

Step 4: Check the result.

#View the information of IS-IS neighbors on Device1.

```

Device1#show isis neighbors
IS-IS Instance 100 Neighbors (Counter 4):
Type System ID Interface State Holdtime Level IETF-NSF Priority Circuit ID
L1-LAN 0000.0000.0002 vlan2 Up 24 sec L1 capable 64 0000.0000.0001.01
L2-LAN 0000.0000.0002 vlan2 Up 23 sec L2 capable 64 0000.0000.0001.01
L1-LAN 0000.0000.0003 vlan2 Up 20 sec L1 capable 64 0000.0000.0001.01
L2-LAN 0000.0000.0004 vlan2 Up 24 sec L2 capable 64 0000.0000.0001.01

```

The pseudo node of Level-1-2 is 0000.0000.0001.01, and Device1 is the DIS of Level-1-2.

---

## Note

- The priority of IS-IS interface is 64 by default. The larger the number the higher the priority.
-

### 57.3.3 Configure IS-IS Inter-area Route Leak

#### Network Requirements

- Leak Level-2 route to Level-1 by configuring inter-layer leak on Level-1-2 device.
- Device1 is a Level-1 router; Device2 is a Level-1-2 router; Device1 and Device2 are in the same area; the area number is 10. Device3 is a Level-2 router, and the area number is 20. Device2 connects the two areas.

#### Network Topology

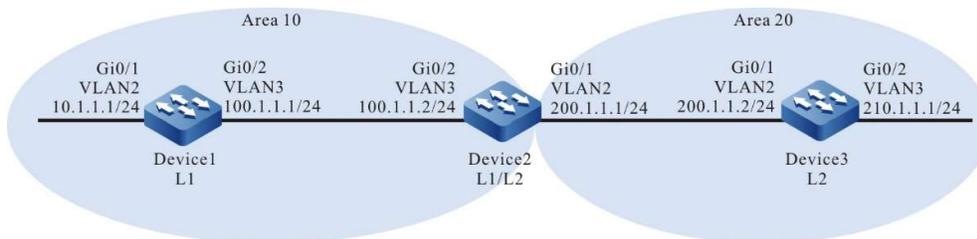


Figure 2 Network Topology for Inter-layer Leak of IS-IS

#### Configuration Steps

Step 1: Configure IP addresses for the ports. (Omitted)

Step 2: Configure IS-IS and enable the this process on the interface.

#On Device1, configure IS-IS process 100, area number 10 and type Level-1, and enable this process on the interface.

```
Device1#configure terminal
Device1(config)#router isis 100
Device1(config-isis)#net 10.0000.0000.0001.00
Device1(config-isis)#is-type level-1
Device1(config-isis)#metric-style wide
Device1(config-isis)#exit
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ip router isis 100
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan3
Device1(config-if-vlan3)#ip router isis 100
Device1(config-if-vlan3)#exit
```

#On Device2, configure IS-IS process 100, area number 10 and type Level-1-2, and enable this process on the interface.

```
Device2#configure terminal
Device2(config)#router isis 100
Device2(config-isis)#net 10.0000.0000.0002.00
Device2(config-isis)#metric-style wide
Device2(config-isis)#exit
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ip router isis 100
Device2(config-if-vlan2)#exit
Device2(config)#interface vlan3
Device2(config-if-vlan3)#ip router isis 100
```

```
Device2(config-if-vlan3)#exit
```

#On Device3, configure IS-IS process 100, area number 20 and type Level-2, and enable this process on the interface.

```
Device3#configure terminal
Device3(config)#router isis 100
Device3(config-isis)#net 20.0000.0000.0003.00
Device3(config-isis)#is-type level-2
Device3(config-isis)#metric-style wide
Device3(config-isis)#exit
Device3(config)#interface vlan2
Device3(config-if-vlan2)#ip router isis 100
Device3(config-if-vlan2)#exit
Device3(config)#interface vlan3
Device3(config-if-vlan3)#ip router isis 100
Device3(config-if-vlan3)#exit
```

#View the routing information of Device1.

```
Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
i 0.0.0.0/0 [115/10] via 100.1.1.2, 17:44:09, vlan3
C 10.1.1.0/24 is directly connected, 16:56:18, vlan2
C 100.1.1.0/24 is directly connected, 18:37:57, vlan3
C 127.0.0.0/8 is directly connected, 284:02:13, lo0
i 200.1.1.0/24 [115/20] via 100.1.1.2, 17:44:09, vlan3
```

```
Device1#show isis ipv4 route
IS-IS Instance 100, VRF Kernel, IPv4 routes table (Counter 4):
L1 0.0.0.0/0, flags none, metric 10, from learned, installed
   via 100.1.1.2, vlan3, neighbor 0000.0000.0002
L1 10.1.1.0/24, flags none, metric 10, from network connected
   via 0.0.0.0, vlan2
L1 100.1.1.0/24, flags none, metric 10, from network connected
   via 0.0.0.0, vlan3
L1 200.1.1.0/24, flags none, metric 20, from learned, installed
   via 100.1.1.2, vlan3, neighbor 0000.0000.0002
```

```
Device1#show isis database detail
IS-IS Instance 100 Level-1 Link State Database (Counter 3, LSP-MTU 1492):
LSPID          LSP Seq Num  LSP Checksum  LSP Holdtime  Length  ATT/P/OL
0000.0000.0001.00-00* 0x0000007E  0xD5DA      1067         71     0/0/0
  NLPID:      IPv4
  Area Address: 10
  IP Address: 100.1.1.1
  Metric: 10   IS-Extended 0000.0000.0001.01
  Metric: 10   IP-Extended 10.1.1.0/24
  Metric: 10   IP-Extended 100.1.1.0/24
0000.0000.0001.01-00* 0x00000073  0xAAAF      471         51     0/0/0
  Metric: 0    IS-Extended 0000.0000.0001.00
  Metric: 0    IS-Extended 0000.0000.0002.00
0000.0000.0002.00-00 0x00000081  0x5926      887         71     1/0/0
  NLPID:      IPv4
  Area Address: 10
  IP Address: 200.1.1.1
  Metric: 10   IS-Extended 0000.0000.0001.01
  Metric: 10   IP-Extended 100.1.1.0/24
  Metric: 10   IP-Extended 200.1.1.0/24
```

There is a default route in the routing table. The next hop is Device2. There is no Level-2 route advertised by Device3.

#View the routing information of Device 2.

```
Device2#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
i 10.1.1.0/24 [115/20] via 100.1.1.1, 16:58:26, vlan3
C 100.1.1.0/24 is directly connected, 18:39:58, vlan3
C 127.0.0.0/8 is directly connected, 20:16:34, lo0
C 200.1.1.0/24 is directly connected, 18:39:37, vlan2
i 210.1.1.0/24 [115/20] via 200.1.1.2, 16:57:56, vlan2
```

```
Device2#show isis ipv4 route
IS-IS Instance 100, VRF Kernel, IPv4 routes table (Counter 4):
L1 10.1.1.0/24, flags none, metric 20, from learned, installed
   via 100.1.1.1, vlan3, neighbor 0000.0000.0001
L1 100.1.1.0/24, flags none, metric 10, from network connected
   via 0.0.0.0, vlan3
L1 200.1.1.0/24, flags none, metric 10, from network connected
   via 0.0.0.0, vlan2
L2 210.1.1.0/24, flags none, metric 20, from learned, installed
   via 200.1.1.2, vlan2, neighbor 0000.0000.0003
```

```
Device2#show isis database detail
IS-IS Instance 100 Level-1 Link State Database (Counter 3, LSP-MTU 1492):
LSPID      LSP Seq Num LSP Checksum LSP Holdtime Length ATT/P/OL
0000.0000.0001.00-00 0x0000007E 0xD5DA      507          71 0/0/0
NLPID:     IPv4
Area Address: 10
IP Address: 100.1.1.1
Metric: 10 IS-Extended 0000.0000.0001.01
Metric: 10 IP-Extended 10.1.1.0/24
Metric: 10 IP-Extended 100.1.1.0/24
0000.0000.0001.01-00 0x00000074 0xA8B0      799          51 0/0/0
Metric: 0  IS-Extended 0000.0000.0001.00
Metric: 0  IS-Extended 0000.0000.0002.00
0000.0000.0002.00-00* 0x00000082 0x5727     1146          71 1/0/0
NLPID:     IPv4
Area Address: 10
IP Address: 200.1.1.1
Metric: 10 IS-Extended 0000.0000.0001.01
Metric: 10 IP-Extended 100.1.1.0/24
Metric: 10 IP-Extended 200.1.1.0/24
```

```
IS-IS Instance 100 Level-2 Link State Database (Counter 3, LSP-MTU 1492):
LSPID      LSP Seq Num LSP Checksum LSP Holdtime Length ATT/P/OL
0000.0000.0002.00-00* 0x00000081 0x84C0     1047          79 0/0/0
NLPID:     IPv4
Area Address: 10
IP Address: 200.1.1.1
Metric: 10 IS-Extended 0000.0000.0003.01
Metric: 20 IP-Extended 10.1.1.0/24
Metric: 10 IP-Extended 100.1.1.0/24
Metric: 10 IP-Extended 200.1.1.0/24
0000.0000.0003.00-00 0x00000315 0x9DC7      543          71 0/0/0
NLPID:     IPv4
Area Address: 20
IP Address: 210.1.1.1
Metric: 10 IS-Extended 0000.0000.0003.01
Metric: 10 IP-Extended 200.1.1.0/24
Metric: 10 IP-Extended 210.1.1.0/24
0000.0000.0003.01-00 0x00000070 0xBF97      526          51 0/0/0
Metric: 0  IS-Extended 0000.0000.0002.00
Metric: 0  IS-Extended 0000.0000.0003.00
```

Device2 includes Level-1 and Level-2 routes.

#View the routing information of Device3 which includes the Level-1 route advertised by Device1.

```
Device3#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
```

U - Per-user Static route  
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

```
i 10.1.1.0/24 [115/30] via 200.1.1.1, 16:59:29, vlan2
i 100.1.1.0/24 [115/20] via 200.1.1.1, 17:47:29, vlan2
C 127.0.0.0/8 is directly connected, 945:29:12, lo0
C 200.1.1.0/24 is directly connected, 18:40:27, vlan2
C 210.1.1.0/24 is directly connected, 16:59:04, vlan3
```

```
Device3#show isis ipv4 route
IS-IS Instance 100, VRF Kernel, IPv4 routes table (Counter 4):
L2 10.1.1.0/24, flags none, metric 30, from learned, installed
   via 200.1.1.1, vlan2, neighbor 0000.0000.0002
L2 100.1.1.0/24, flags none, metric 20, from learned, installed
   via 200.1.1.1, vlan2, neighbor 0000.0000.0002
L2 200.1.1.0/24, flags none, metric 10, from network connected
   via 0.0.0.0, vlan2
L2 210.1.1.0/24, flags none, metric 10, from network connected
   via 0.0.0.0, vlan3
```

```
Device3#show isis database detail
IS-IS Instance 100 Level-2 Link State Database (Counter 3, LSP-MTU 1492):
LSPID      LSP Seq Num  LSP Checksum  LSP Holdtime  Length  ATT/P/OL
0000.0000.0002.00-00  0x00000081  0x84C0      880          79     0/0/0
  NLPID:    IPv4
  Area Address: 10
  IP Address: 200.1.1.1
  Metric: 10   IS-Extended 0000.0000.0003.01
  Metric: 20   IP-Extended 10.1.1.0/24
  Metric: 10   IP-Extended 100.1.1.0/24
  Metric: 10   IP-Extended 200.1.1.0/24
0000.0000.0003.00-00* 0x00000316  0x9BC8      1197         71     0/0/0
  NLPID:    IPv4
  Area Address: 20
  IP Address: 210.1.1.1
  Metric: 10   IS-Extended 0000.0000.0003.01
  Metric: 10   IP-Extended 200.1.1.0/24
  Metric: 10   IP-Extended 210.1.1.0/24
0000.0000.0003.01-00* 0x00000070  0xBF97      359          51     0/0/0
  Metric: 0    IS-Extended 0000.0000.0002.00
  Metric: 0    IS-Extended 0000.0000.0003.00
```

Step 3: Configure inter-layer leak.

#Configure inter-layer leak on Device2.

```
Device2(config)#router isis 100
Device2(config-isis)#address-family ipv4 unicast
Device2(config-isis-af)#propagate level-2 into level-1
Device2(config-isis-af)#exit
Device2(config-isis)#exit
```

Step 4: Check the result.

#View the routing information of Device1.

```
Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

i 0.0.0.0/0 [115/10] via 100.1.1.2, 17:44:09, vlan3
C 10.1.1.0/24 is directly connected, 16:56:18, vlan2
C 100.1.1.0/24 is directly connected, 18:37:57, vlan3
C 127.0.0.0/8 is directly connected, 284:02:13, lo0
```

```
i 200.1.1.0/24 [115/20] via 100.1.1.2, 17:44:09, vlan3
i 210.1.1.0/24 [115/30] via 100.1.1.2, 00:00:01, vlan3
```

```
Device1#show isis ipv4 route
L1 0.0.0.0/0, flags none, metric 10, from learned, installed
  via 100.1.1.2, vlan3, neighbor 0000.0000.0002
L1 100.1.1.0/24, flags none, metric 10, from network connected
  via 0.0.0.0, vlan3
L1 200.1.1.0/24, flags none, metric 20, from learned, installed
  via 100.1.1.2,vlan3, neighbor 0000.0000.0002
L1 210.1.1.0/24, flags inter-area, metric 30, from learned, installed
  via 100.1.1.2, vlan3, neighbor 0000.0000.0002
```

```
Device1#show isis database detail
IS-IS Instance 100 Level-1 Link State Database (Counter 3, LSP-MTU 1492):
LSPID      LSP Seq Num  LSP Checksum  LSP Holdtime  Length  ATT/P/OL
0000.0000.0001.00-00* 0x0000007F  0xD3DB      668          71    0/0/0
NLPID:     IPv4
Area Address: 10
IP Address: 100.1.1.1
Metric: 10  IS-Extended 0000.0000.0001.01
Metric: 10  IP-Extended 100.1.1.0/24
Metric: 10  IP-Extended 100.1.1.0/24
0000.0000.0001.01-00* 0x00000075  0xA6B1      995          51    0/0/0
Metric: 0   IS-Extended 0000.0000.0001.00
Metric: 0   IS-Extended 0000.0000.0002.00
0000.0000.0002.00-00 0x00000083  0x4DA6      984          79    1/0/0
NLPID:     IPv4
Area Address: 10
IP Address: 200.1.1.1
Metric: 10  IS-Extended 0000.0000.0001.01
Metric: 10  IP-Extended 100.1.1.0/24
Metric: 10  IP-Extended 200.1.1.0/24
Metric: 20  IP-Extended ia 210.1.1.0/24
```

In addition to default route, Device1 learns the Level-2 route advertised by Device3.

### 57.3.4 IS-IS route redistribution

#### Network Requirements

- Configure redistribution to import external routes into IS-IS for network interconnection between devices.
- Both Device1 and Device2 are Level-2 routers. Configure IS-IS, with the area number being 10. Configure OSPF for Device2 and Device3. On Device2, redistribute OSPF route to IS-IS through configuration.

#### Network Topology

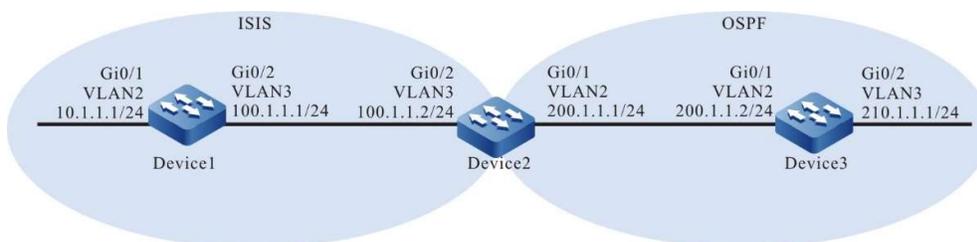


Figure 3 Network Topology for IS-IS Route Redistribution

#### Configuration Steps

Step 1: Configure IP addresses for the ports. (Omitted)

Step 2: Configure IS-IS and enable the this process on the interface.

#On Device1, configure IS-IS process 100, area number 10 and type Level-2, and enable this process on the interface.

```
Device1#configure terminal
Device1(config)#router isis 100
Device1(config-isis)#net 10.0000.0000.0001.00
Device1(config-isis)#is-type level-2
Device1(config-isis)#metric-style wide
Device1(config-isis)#exit
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ip router isis 100
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan3
Device1(config-if-vlan3)#ip router isis 100
Device1(config-if-vlan3)#exit
```

#On Device2, configure IS-IS process 100, area number 10 and type Level-1-2, and enable this process on the interface.

```
Device2#configure terminal
Device2(config)#router isis 100
Device2(config-isis)#net 10.0000.0000.0002.00
Device2(config-isis)#is-type level-2
Device2(config-isis)#metric-style wide
Device2(config-isis)#exit
Device2(config)#interface vlan3
Device2(config-if-vlan3)#ip router isis 100
Device2(config-if-vlan3)#exit
```

Step 3: Configure OSPF.

#Configure Device2.

```
Device2(config)#router ospf 100
Device2(config-ospf)#network 200.1.1.0 0.0.0.255 area 0
Device2(config-ospf)#exit
```

#Configure Device3.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#network 210.1.1.0 0.0.0.255 area 0
Device3(config-ospf)#network 200.1.1.0 0.0.0.255 area 0
Device3(config-ospf)#exit
```

#View the routing table of Device1. Device1 fails to learn the OSPF route redistributed by Device2.

```
Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 10.1.1.0/24 is directly connected, 00:58:39, vlan2
C 100.1.1.0/24 is directly connected, 06:55:35, vlan3
C 127.0.0.0/8 is directly connected, 603:06:22, lo0

Device1#show isis ipv4 route
IS-IS Instance 100, VRF Kernel, IPv4 routes table (Counter 2):
L2 10.1.1.0/24, flags none, metric 10, from network connected
```

```
via 0.0.0.0, vlan2
L2 100.1.1.0/24, flags none, metric 10, from network connected
via 0.0.0.0, vlan3
```

```
Device1#show isis database detail
IS-IS Instance 100 Level-2 Link State Database (Counter 3, LSP-MTU 1492):
LSPID      LSP Seq Num LSP Checksum LSP Holdtime Length ATT/P/OL
0000.0000.0001.00-00* 0x00000046 0x489E    1123      71  0/0/0
NLPID:     IPv4
Area Address: 10
IP Address: 100.1.1.1
Metric: 10 IS-Extended 0000.0000.0001.01
Metric: 10 IP-Extended 10.1.1.0/24
Metric: 10 IP-Extended 100.1.1.0/24
0000.0000.0001.01-00* 0x00000045 0x097D    1103      51  0/0/0
Metric: 0 IS-Extended 0000.0000.0001.00
Metric: 0 IS-Extended 0000.0000.0002.00
0000.0000.0002.00-00 0x000000CB 0xEEA6    679      63  0/0/0
NLPID:     IPv4
Area Address: 10
IP Address: 100.1.1.2
Metric: 10 IS-Extended 0000.0000.0001.01
Metric: 10 IP-Extended 100.1.1.0/24
```

#View the routing table of Device 2. Device2 learns ISIS and OSPF route.

```
Device2#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
U - Per-user Static route
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
i 10.1.1.0/24 [115/20] via 100.1.1.1, 15:45:37, vlan3
C 100.1.1.0/24 is directly connected, 22:38:58, vlan3
C 127.0.0.0/8 is directly connected, 300:03:03, lo0
C 200.1.1.0/24 is directly connected, 22:38:58, vlan2
O 210.1.1.1/32 [110/2] via 200.1.1.2, 15:43:35, vlan2
```

```
Device2#show isis ipv4 route
IS-IS Instance 100, VRF Kernel, IPv4 routes table (Counter 2):
L2 10.1.1.0/24, flags none, metric 20, from learned, installed
via 100.1.1.1, vlan3, neighbor 0000.0000.0001
L2 100.1.1.0/24, flags none, metric 10, from network connected
via 0.0.0.0, vlan3
```

```
Device2#show isis database detail
IS-IS Instance 100 Level-2 Link State Database (Counter 3, LSP-MTU 1492):
LSPID      LSP Seq Num LSP Checksum LSP Holdtime Length ATT/P/OL
0000.0000.0001.00-00 0x00000046 0x489E    911      71  0/0/0
NLPID:     IPv4
Area Address: 10
IP Address: 100.1.1.1
Metric: 10 IS-Extended 0000.0000.0001.01
Metric: 10 IP-Extended 10.1.1.0/24
Metric: 10 IP-Extended 100.1.1.0/24
0000.0000.0001.01-00 0x00000045 0x097D    892      51  0/0/0
Metric: 0 IS-Extended 0000.0000.0001.00
Metric: 0 IS-Extended 0000.0000.0002.00
0000.0000.0002.00-00* 0x000000CB 0xEEA6    467      63  0/0/0
NLPID:     IPv4
Area Address: 10
IP Address: 100.1.1.2
Metric: 10 IS-Extended 0000.0000.0001.01
Metric: 10 IP-Extended 100.1.1.0/24
```

Step 4: Configure IS-IS to redistribute OSPF route.

#On Device2, redistribute OSPF route to Level-2.

```

Device2(config)#router isis 100
Device2(config-isis)#address-family ipv4 unicast
Device2(config-isis-af)#redistribute ospf 100 level-2
Device2(config-isis-af)#exit
Device2(config-isis)#exit

```

Step 5: Check the result.

#View the routing information of Device1. Device1 learns the OSPF route redistributed by Device2.

```

Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

```

```

C 10.1.1.0/24 is directly connected, 16:47:30, vlan2
C 100.1.1.0/24 is directly connected, 22:44:27, vlan3
C 127.0.0.0/8 is directly connected, 618:55:13, lo0
i 200.1.1.0/24 [115/10] via 100.1.1.2, 00:00:05, vlan3
i 210.1.1.1/32 [115/10] via 100.1.1.2, 00:00:05, vlan3

```

```

Device1#show isis ipv4 route
IS-IS Instance 100, VRF Kernel, IPv4 routes table (Counter 4):
L2 10.1.1.0/24, flags none, metric 10, from network connected
   via 0.0.0.0, vlan2
L2 100.1.1.0/24, flags none, metric 10, from network connected
   via 0.0.0.0, vlan3
L2 200.1.1.0/24, flags none, metric 10, from learned, installed
   via 100.1.1.2, vlan3, neighbor 0000.0000.0002
L2 210.1.1.1/32, flags none, metric 10, from learned, installed
   via 100.1.1.2, vlan3, neighbor 0000.0000.0002

```

```

Device1#show isis database detail
IS-IS Instance 100 Level-2 Link State Database (Counter 3, LSP-MTU 1492):
LSPID      LSP Seq Num LSP Checksum LSP Holdtime Length ATT/P/OL
0000.0000.0001.00-00* 0x00000046 0x489E    626      71  0/0/0
NLPID:    IPv4
Area Address: 10
IP Address: 100.1.1.1
Metric: 10   IS-Extended 0000.0000.0001.01
Metric: 10   IP-Extended 10.1.1.0/24
Metric: 10   IP-Extended 100.1.1.0/24
0000.0000.0001.01-00* 0x00000045 0x097D    606      51  0/0/0
Metric: 0    IS-Extended 0000.0000.0001.00
Metric: 0    IS-Extended 0000.0000.0002.00
0000.0000.0002.00-00 0x000000CD 0xC6E2    1184     80  0/0/0
NLPID:    IPv4
Area Address: 10
IP Address: 100.1.1.2
Metric: 10   IS-Extended 0000.0000.0001.01
Metric: 10   IP-Extended 100.1.1.0/24
Metric: 0    IP-Extended 200.1.1.0/24
Metric: 0    IP-Extended 210.1.1.1/32

```

Device1 learns the OSPF route redistributed.

### 57.3.5 Configure IS-IS Neighbor Authentication

#### Network Requirements

- Enable authentication on the interface to establish neighbors between devices configured with the same password.
- Device1 is a Level-1 router; Device2 is a Level-1-2 router; Device1 and Device2 are in

the same area; the area number is 10. Device3 is a Level-2 router, and the area number is 20. Device2 connects the two areas.

### Network Topology

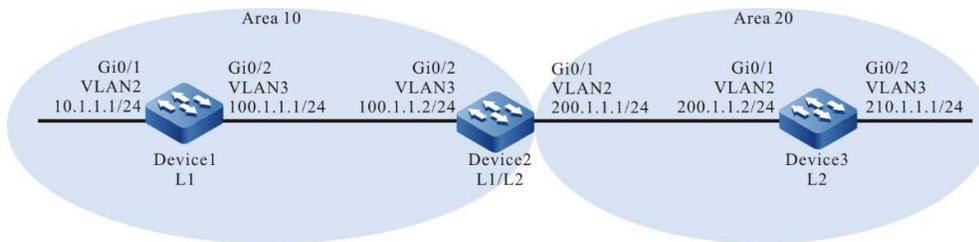


Figure 4 Network Topology for IS-IS Neighbor Authentication

### Configuration Steps

Step 1: Configure IP addresses for the ports. (Omitted)

Step 2: Configure IS-IS and enable the this process on the interface.

#On Device1, configure IS-IS process 100, area number 10 and type Level-1, and enable this process on the interface.

```
Device1#configure terminal
Device1(config)#router isis 100
Device1(config-isis)#net 10.0000.0000.0001.00
Device1(config-isis)#is-type level-1
Device1(config-isis)#metric-style wide
Device1(config-isis)#exit
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ip router isis 100
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan3
Device1(config-if-vlan3)#ip router isis 100
Device1(config-if-vlan3)#exit
```

#On Device2, configure IS-IS process 100, area number 10 and type Level-1-2, and enable this process on the interface.

```
Device2#configure terminal
Device2(config)#router isis 100
Device2(config-isis)#net 10.0000.0000.0002.00
Device2(config-isis)#metric-style wide
Device2(config-isis)#exit
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ip router isis 100
Device2(config-if-vlan2)#exit
Device2(config)#interface vlan3
Device2(config-if-vlan3)#ip router isis 100
Device2(config-if-vlan3)#exit
```

#On Device3, configure IS-IS process 100, area number 20 and type Level-2, and enable this process on the interface.

```
Device3#configure terminal
Device3(config)#router isis 100
Device3(config-isis)#net 20.0000.0000.0003.00
Device3(config-isis)#is-type level-2
```

```
Device3(config-isis)#metric-style wide
Device3(config-isis)#exit
Device3(config)#interface vlan2
Device3(config-if-vlan2)#ip router isis 100
Device3(config-if-vlan2)#exit
Device3(config)#interface vlan3
Device3(config-if-vlan3)#ip router isis 100
Device3(config-if-vlan3)#exit
```

#View the information of IS-IS neighbors on Device1.

```
Device1#show isis neighbors
IS-IS Instance 100 Neighbors (Counter 1):
Type System ID Interface State Holdtime Level IETF-NSF Priority Circuit ID
L1-LAN 0000.0000.0002 vlan3 Up 29 sec L1 capable 64 0000.0000.0001.01
```

#View the information of IS-IS neighbors on Device2.

```
Device2#show isis neighbors
IS-IS Instance 100 Neighbors (Counter 2):
Type System ID Interface State Holdtime Level IETF-NSF Priority Circuit ID
L2-LAN 0000.0000.0003 vlan2 Up 9 sec L2 capable 64 0000.0000.0003.01
L1-LAN 0000.0000.0001 vlan3 Up 7 sec L1 capable 64 0000.0000.0001.01
```

#View the information of IS-IS neighbors on Device 3.

```
Device3#show isis neighbors
IS-IS Instance 100 Neighbors (Counter 1):
Type System ID Interface State Holdtime Level IETF-NSF Priority Circuit ID
L2-LAN 0000.0000.0002 vlan2 Up 24 sec L2 capable 64 0000.0000.0003.01
```

Step 3: Configure authentication.

#Configure MD5 authentication on the interface of Device2, with the password being admin.

```
Device2(config)#interface vlan2
Device2(config-if-vlan2)#isis authentication mode md5
Device2(config-if-vlan2)#isis authentication key 0 admin
Device2(config-if-vlan2)#exit
Device2(config)#interface vlan3
Device2(config-if-vlan3)#isis authentication mode md5
Device2(config-if-vlan3)#isis authentication key 0 admin
Device2(config-if-vlan3)#exit
```

#View the IS-IS neighbors on Device2.

```
Device2#show isis neighbors
IS-IS Instance 100 Neighbors (Counter 0):
Type System ID Interface State Holdtime Level IETF-NSF Priority Circuit ID
```

At this moment, no authentication has been configured on Device1 and Device3, and there is no ISIS neighbor on Device2.

#Configure MD5 authentication on the vlan3 interface of Device1, with the password being admin.

```
Device1(config)#interface vlan3
Device1(config-if-vlan3)#isis authentication mode md5
Device1(config-if-vlan3)#isis authentication key 0 admin
Device1(config-if-vlan3)#exit
```

#Configure MD5 authentication on the vlan2 interface of Device3, with the password being admin.

```
Device3(config)#interface vlan2
Device3(config-if-vlan2)#isis authentication mode md5
Device3(config-if-vlan2)#isis authentication key 0 admin
Device3(config-if-vlan2)#exit
```

Step 4: Check the result.

#View the information of IS-IS neighbors on Device1.

```
Device1#show isis neighbors
IS-IS Instance 100 Neighbors (Counter 1):
Type System ID Interface State Holdtime Level IETF-NSF Priority Circuit ID
L1-LAN 0000.0000.0002 vlan3 Up 29 sec L1 capable 64 0000.0000.0001.01
```

According to the result, ISIS neighbor has been successfully established between Device1 and Device2. This means the authentication has succeeded.

#View the information of IS-IS neighbors on Device2.

```
Device2#show isis neighbors
IS-IS Instance 100 Neighbors (Counter 2):
Type System ID Interface State Holdtime Level IETF-NSF Priority Circuit ID
L2-LAN 0000.0000.0003 vlan2 Up 9 sec L2 capable 64 0000.0000.0003.01
L1-LAN 0000.0000.0001 vlan3 Up 7 sec L1 capable 64 0000.0000.0001.01
```

According to the result, ISIS neighbor has been successfully established between Device2 and Device1 & Device3. This means the authentication has succeeded.

#View the information of IS-IS neighbors on Device 3.

```
Device3#show isis neighbors
IS-IS Instance 100 Neighbors (Counter 1):
Type System ID Interface State Holdtime Level IETF-NSF Priority Circuit ID
L2-LAN 0000.0000.0002 vlan2 Up 24 sec L2 capable 64 0000.0000.0003.01
```

According to the result, ISIS neighbor has been successfully established between Device3 and Device2. This means the authentication has succeeded.

#View the routing information of Device2. It can normally receive the routes advertised by Device1 and Device3.

```
Device2#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
U - Per-user Static route
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
i 10.1.1.0/24 [115/20] via 100.1.1.1, 16:58:26, vlan3
C 100.1.1.0/24 is directly connected, 18:39:58, vlan3
C 127.0.0.0/8 is directly connected, 20:16:34, lo0
C 200.1.1.0/24 is directly connected, 18:39:37, vlan2
i 210.1.1.0/24 [115/20] via 200.1.1.2, 16:57:56, vlan2
```

```
Device2#show isis ipv4 route
IS-IS Instance 100, VRF Kernel, IPv4 routes table (Counter 4):
L1 10.1.1.0/24, flags none, metric 20, from learned, installed
via 100.1.1.1, vlan3, neighbor 0000.0000.0001
L1 100.1.1.0/24, flags none, metric 10, from network connected
via 0.0.0.0, vlan3
L1 200.1.1.0/24, flags none, metric 10, from network connected
via 0.0.0.0, vlan2
L2 210.1.1.0/24, flags none, metric 20, from learned, installed
via 200.1.1.2, vlan2, neighbor 0000.0000.0003
```

## 57.3.6 Configure Coordination of IS-IS with BFD

### Network Requirements

- Configure BFD association between devices. When the main line fails, the service can quickly switch to the backup line.
- Device1, Device2, and Device3 are all Level-2 routers and in the same area, with the area number being 10. Configure BFD on Device1 and Device3 to establish a session. When the intermediate line between Device1 and Device3 is disconnected under abnormal conditions, Device1 can quickly switch and learn the 10.1.1.1/24 route from Device2.

### Network Topology

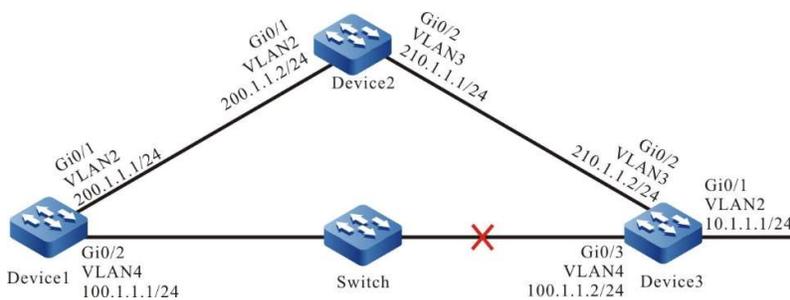


Figure 5 Network Topology for Coordination of IS-IS with BFD

### Configuration Steps

Step 1: Configure IP addresses for the ports. (Omitted)

Step 2: Configure IS-IS and enable the this process on the interface.

#On Device1, configure IS-IS process 100, area number 10 and type Level-2, and enable this process on the interface.

```
Device1#configure terminal
Device1(config)#router isis 100
Device1(config-isis)#net 10.0000.0000.0001.00
Device1(config-isis)#is-type level-2
Device1(config-isis)#metric-style wide
Device1(config-isis)#exit
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ip router isis 100
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan4
Device1(config-if-vlan4)#ip router isis 100
Device1(config-if-vlan4)#exit
```

#On Device2, configure IS-IS process 100, area number 10 and type Level-2, and enable this process on the interface.

```
Device2#configure terminal
Device2(config)#router isis 100
Device2(config-isis)#net 10.0000.0000.0002.00
Device2(config-isis)#is-type level-2
```

```

Device2(config-isis)#metric-style wide
Device2(config-isis)#exit
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ip router isis 100
Device2(config-if-vlan2)#exit
Device2(config)#interface vlan3
Device2(config-if-vlan3)#ip router isis 100
Device2(config-if-vlan3)#exit

```

#On Device3, configure IS-IS process 100, area number 10 and type Level-2, and enable this process on the interface.

```

Device3#configure terminal
Device3(config)#router isis 100
Device3(config-isis)#net 10.0000.0000.0003.00
Device3(config-isis)#is-type level-2
Device3(config-isis)#metric-style wide
Device3(config-isis)#exit
Device3(config)#interface vlan2
Device3(config-if-vlan2)#ip router isis 100
Device3(config-if-vlan2)#exit
Device3(config)#interface vlan3
Device3(config-if-vlan3)#ip router isis 100
Device3(config-if-vlan3)#exit
Device3(config)#interface vlan4
Device3(config-if-vlan4)#ip router isis 100
Device3(config-if-vlan4)#exit

```

#View the routing information of Device1 which prefers the route 10.1.1.0/24 advertised by Device3.

```

Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

i 10.1.1.0/24 [115/20] via 100.1.1.2, 00:00:15, vlan4
C 100.1.1.0/24 is directly connected, 00:09:15, vlan4
C 127.0.0.0/8 is directly connected, 253:58:17, lo0
C 200.1.1.0/24 is directly connected, 00:11:29, vlan2
i 210.1.1.0/24 [115/20] via 100.1.1.2, 00:00:15, vlan4
  [115/20] via 200.1.1.2, 00:00:15, vlan2
Device1#show isis ipv4 route
IS-IS Instance 100, VRF Kernel, IPv4 routes table (Counter 4):
L2 10.1.1.0/24, flags none, metric 20, from learned, installed
   via 100.1.1.2, vlan4, neighbor 0000.0000.0003
L2 100.1.1.0/24, flags none, metric 10, from network connected
   via 0.0.0.0, vlan4
L2 200.1.1.0/24, flags none, metric 10, from network connected
   via 0.0.0.0, vlan2
L2 210.1.1.0/24, flags none, metric 20, from learned, installed
   via 100.1.1.2, vlan4, neighbor 0000.0000.0003
   via 200.1.1.2, vlan2, neighbor 0000.0000.0002

```

### Step 3: Configure BFD.

#Enable BFD on the interface of Device1.

```

Device1(config)#bfd fast-detect
Device1(config)#interface vlan4
Device1(config-if-vlan4)#isis bfd
Device1(config-if-vlan4)#exit
#Enable BFD on the interface of Device3.
Device3(config)#bfd fast-detect
Device3(config)#interface vlan4
Device3(config-if-vlan4)#isis bfd
Device3(config-if-vlan4)#exit

```

#View the BFD information of Device1.

```
Device1#show bfd session
OurAddr      NeighAddr      LD/RD      State
100.1.1.2    100.1.1.1     1/1       UP
Holddown     interface
5000         vlan4
```

Step 4: Check the result.

#When the line between Device1 and Device3 fails, BFD will quickly identify the failure and notify ISIS which will switch route to Device2 for communication. View the routing table on Device1.

```
Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
U - Per-user Static route
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
i 10.1.1.0/24 [115/30] via 200.1.1.2, 00:00:14, vlan2
C 127.0.0.0/8 is directly connected, 112:55:25, lo0
C 200.1.1.0/24 is directly connected, 101:20:08, vlan2
```

```
Device1#show isis ipv4 route
IS-IS Instance 100, VRF Kernel, IPv4 routes table (Counter 2):
L2 10.1.1.0/24, flags none, metric 30, from I earned, installed
   via 200.1.1.2, vlan2, neighbor 0000.0000.0003
L2 200.1.1.0/24, flags none, metric 20, from network connected
   via 0.0.0.0, vlan2
```

#According to the result, for the data flow from Device1 to the network segment 10.1.1.0/24, priority is given to Device2.

### 57.3.7 Configure ISIS FRR

#### Network Requirements

- All devices are configured with ISIS protocol.
- Device1 learns the ISIS route 192.168.1.1/32 from Device2 and Device3 at the same time, and first uses the lines between it and Device3 to forward packets. Likewise, Device3 learns the ISIS route 100.1.1.1/32 from Device1 and Device2, and prefers to use the lines between it and Device1 to forward packets.
- Enable ISIS FRR on Device1 and Device3. When the lines between Device1 and Device3 fail, the service can quickly switch to Device2 for communication.

#### Network Topology

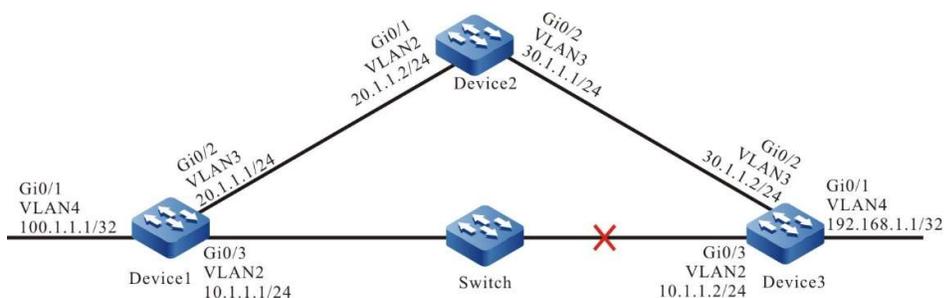


Figure 6 Network Topology for Configuring ISIS FRR

### Configuration Steps

Step 1: Configures IP addresses for the ports. (Omitted)

Step 2: Configure IS-IS and enable the this process on the interface.

#On Device1, configure IS-IS process 100, area number 10 and type Level-2, and enable this process on the interface.

```
Device1#configure terminal
Device1(config)#router isis 100
Device1(config-isis)#net 10.0000.0000.0001.00
Device1(config-isis)#is-type level-2
Device1(config-isis)#metric-style wide
Device1(config-isis)#exit
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ip router isis 100
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan3
Device1(config-if-vlan3)#ip router isis 100
Device1(config-if-vlan3)#exit
Device1(config)#interface loopback 0
Device1(config-if-loopback0)#ip router isis 100
Device1(config-if-loopback0)#exit
```

#On Device2, configure IS-IS process 100, area number 10 and type Level-2, and enable this process on the interface.

```
Device2#configure terminal
Device2(config)#router isis 100
Device2(config-isis)#net 10.0000.0000.0002.00
Device2(config-isis)#is-type level-2
Device2(config-isis)#metric-style wide
Device2(config-isis)#exit
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ip router isis 100
Device2(config-if-vlan2)#exit
Device2(config)#interface vlan3
Device2(config-if-vlan3)#ip router isis 100
Device2(config-if-vlan3)#exit
```

#On Device3, configure IS-IS process 100, area number 10 and type Level-2, and enable this process on the interface.

```
Device3#configure terminal
Device3(config)#router isis 100
Device3(config-isis)#net 10.0000.0000.0003.00
Device3(config-isis)#is-type level-2
Device3(config-isis)#metric-style wide
Device3(config-isis)#exit
Device3(config)#interface vlan2
Device3(config-if-vlan2)#ip router isis 100
Device3(config-if-vlan2)#exit
Device3(config)#interface vlan3
Device3(config-if-vlan3)#ip router isis 100
Device3(config-if-vlan3)#exit
Device3(config)#interface loopback 0
Device3(config-if-loopback0)#ip router isis 100
Device3(config-if-loopback0)#exit
```

Step 3: Configure routing policy.

#On Device1, configure route-map to invoke ACL to match 192.168.1.1/32 only, and filter other networks.

The route matching the match rule applies the backup next hop interface vlan3. The next hop address is 20.1.1.2.

```
Device1(config)#ip access-list standard 1
Device1(config-std-nacl)#permit 192.168.1.1 0.0.0.0
Device1(config-std-nacl)#exit
Device1(config)#route-map ipfir_isis
Device1(config-route-map)#match ip address 1
Device1(config-route-map)#set fast-reroute backup-interface vlan3 backup-nexthop 20.1.1.2
Device1(config-route-map)#exit
```

#On Device3, configure route-map to invoke ACL to match 100.1.1.1/32 only, and filter other networks.

The route matching the match rule applies the backup next hop interface vlan3. The next hop address is 30.1.1.1.

```
Device3(config)#ip access-list standard 1
Device3(config-std-nacl)#permit 100.1.1.1 0.0.0.0
Device3(config-std-nacl)#exit
Device3(config)#route-map ipfir_isis
Device3(config-route-map)#match ip address 1
Device3(config-route-map)#set fast-reroute backup-interface vlan3 backup-nexthop 30.1.1.1
Device3(config-route-map)#exit
```

#### Step 4: Configure FRR.

#On Device1, enable ISIS FRR.

```
Device1(config)#router isis 100
Device1(config-isis)#address-family ipv4 unicast
Device1(config-isis-af)#ipfir route-map ipfir_isis
Device1(config-isis-af)#exit-address-family
Device1(config-isis)#exit
```

#On Device3, enable ISIS FRR.

```
Device3(config)#router isis 100
Device3(config-isis)#address-family ipv4 unicast
Device3(config-isis-af)#ipfir route-map ipfir_isis
Device3(config-isis-af)#exit-address-family
Device3(config-isis)#exit
```

#### Step 5: Check the result.

#View the routing table of Device1.

```
Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
C 10.1.1.0/24 is directly connected, 00:02:39, vlan2
L 10.1.1.1/32 is directly connected, 00:02:39, vlan2
C 20.1.1.0/24 is directly connected, 06:19:51, vlan3
L 20.1.1.1/32 is directly connected, 06:19:51, vlan3
i 30.1.1.0/24 [115/20] via 20.1.1.2, 00:00:03, vlan3
   [115/20] via 10.1.1.2, 00:00:03, vlan2
C 127.0.0.0/8 is directly connected, 30:54:34, lo0
L 127.0.0.1/32 is directly connected, 30:54:34, lo0
LC 100.1.1.1/32 is directly connected, 02:54:43, loopback0
i 192.168.1.1/32 [115/20] via 10.1.1.2, 00:01:13, vlan2
```

#The FRR table of Device1 shows the route of network 192.168.1.1/32. The next hop interface is vlan3.

```
Device1#show ip frr route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
i 192.168.1.1/32 [115/0] via 20.1.1.2, 00:00:03, vlan3
```

#According to the backup next hop information of Device1, the backup interface of FRR is vlan3.

```
Device1#show nexthop frr detail
Index          : 262
Type           : FRR
Reference Count : 1
Active Path    : master
Nexthop Address : 10.1.1.2
Interface      : vlan2
Interface Vrf  : global
Channel ID     : 10
Link Header Length : 18
Link Header    : 00017abc662b201201010101810000010800
Action        : FORWARDING
Slot          : 0
BK Nexthop Address : 20.1.1.2
BK Interface     : vlan3
BK Interface Vrf : global
BK Channel ID    : 11
BK Link Header Length : 18
BK Link Header   : 00017a455449201201010102810000020800
BK Action       : FORWARDING
BK Slot         : 0
```

Total 1 entries.

#When the lines between Device1 and Device3 fail, it will quickly identify the failures and switch to Device2 for communication. It can be seen from the routing table and FRR table of Device1 that the output interface of the destination network 192.168.1.1/32 in the routing table has switched to the backup interface vlan3.

```
Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 10.1.1.0/24 is directly connected, 00:02:39, vlan2
L 10.1.1.1/32 is directly connected, 00:02:39, vlan2
C 20.1.1.0/24 is directly connected, 06:19:51, vlan3
L 20.1.1.1/32 is directly connected, 06:19:51, vlan3
i 30.1.1.0/24 [115/20] via 20.1.1.2, 00:00:03, vlan3
   [115/20] via 10.1.1.2, 00:00:03, vlan2
C 127.0.0.0/8 is directly connected, 30:54:34, lo0
L 127.0.0.1/32 is directly connected, 30:54:34, lo0
LC 100.1.1.1/32 is directly connected, 02:54:43, loopback0
i 192.168.1.1/32 [115/30] via 20.1.1.2, 00:01:13, vlan3
```

On Device3, it is processed in a manner which is similar to that on Device1.

# 58 IPv6 IS-IS

## 58.1 Overview

The IPv6 routing protocol has the same protocol behaviors as the IS-IS routing protocol except for the IP address structure in the packet. For details, see the overview of IS-IS route.

## 58.2 IPv6 IS-IS function configuration

Table 58 IPv6 IS-IS Function Configuration List

Configuration Task	
Configure Basic Functions of IPv6 IS-IS	Enable IPv6 IS-IS Protocol
	Configure IPv6 IS-IS VRF Attributes
Configure Attributes of IPv6 IS-IS Layer	Configure Attributes of IPv6 IS-IS Layer
Configure IPv6 IS-IS Route Generation	Configure IPv6 IS-IS Default Route
	Configure IPv6 IS-IS Route Redistribution
Configure IPv6 IS-IS Route Control	Configure IPv6 IS-IS Metric Type
	Configure Metric Value of IPv6 IS-IS Interface
	Configure IPv6 IS-IS Administrative Distance
	Configure IPv6 IS-IS Route Summarization
	Configure the Maximum Number of IPv6 IS-IS Load Balancing Entries
	Configure IPv6 IS-IS Inter-layer Route Leak
Configure IPv6 IS-IS Network Optimization	Configure IPv6 IS-IS ATT Bit
	Configure IPv6 IS-IS Interface Priority
	Configure Passive IPv6 IS-IS Interface

Configuration Task	
	Configure Hello Packet Parameters of IPv6 IS-IS
	Configure LSP Packet Parameters of IPv6 IS-IS
	Configure SNP Packet Parameters of IPv6 IS-IS
	Configure SPF Calculation Interval of IPv6 IS-IS
	Configure the Maximum Number of Areas for IPv6 IS-IS
	Configure IPv6 IS-IS Host Name Mapping
	Add IPv6 IS-IS Interface into Mesh Group
Configure IPv6 IS-IS Network Authentication	Configure IPv6 IS-IS Neighbor Authentication
	Configure IPv6 IS-IS Route Authentication
Configure IPv6 IS-IS GR	Configure IPv6 IS-IS GR

## 58.2.1 Configure Basic Functions of IPv6 IS-IS

### Configuration Condition

Before using the IPv6 IS-IS protocol, ensure that:

- The link layer protocol has been configured to ensure normal communication at the link layer.
- Configure address of interface at network layer so that neighbor network nodes are reachable at the network layer.

### Enable IS-IS Protocol

Multiple IPv6 IS-IS processes can run in the system, and each of them is distinguished by process name.

Table 58 Enabling IPv6 IS-IS Protocol

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Create IS-IS process and enter IS-IS configuration mode	<b>router isis</b> [ <i>area-tag</i> ]	Mandatory By default, there is no IS-IS process running in the system, and <i>area-tag</i> is a process name.
Configure network entity title for IS-IS	<b>net</b> <i>entry-title</i>	Mandatory By default, IS-IS doesn't have network entity title.
Return to the global configuration mode	<b>exit</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Enable IPv6 IS-IS protocol on the interface	<b>ipv6 router isis</b> [ <i>area-tag</i> ]	Mandatory By default, IPv6 IS-IS protocol is disabled on the interface.

### Note

IS-IS cannot be run if there is no network entity title.

### Configure IS-IS VRF Attributes

Table 58 Configuring IS-IS VRF Attributes

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the IS-IS configuration mode	<b>router isis</b> [ <i>area-tag</i> ]	-
Configure IS-IS VRF attributes	<b>vrf</b> <i>vrf-name</i>	Optional By default, the IS-IS process is within the global VRF.

## 58.2.2 Configure Attributes of IPv6 IS-IS Layer

### Configuration Condition

Before configuring attributes of IPv6 IS-IS layer, ensure that:

- Configure the IPv6 address of interface so that neighbor nodes are reachable at the network layer.
- Enable the IPv6 IS-IS protocol.

### Configure Attributes of IS-IS Layer

Attributes of IS-IS layer have two types, i.e. global layer attributes and interface layer attributes. Global layer attributes are the categories of IS-IS intermediate system. They are divided into the following three categories:

- Level-1 intermediate system: It has Level-1 link status database only, and can advertise and learn routes in Level-1 area only;
- Level-2 intermediate system: It has Level-2 link status database only, and can advertise and learn routes in Level-2 area only;
- Level-1-2 intermediate system: It has both Level-1 and Level-2 link status databases, and can advertise and learn both Level-1 and Level-2 routes. It is an interconnecting device in Level-1 and Level-2 area.

The IS-IS interface layer attributes also have three types:

- Level-1 interface: It can send and receive Level-1 packets of IS-IS protocol only, and can establish Level-1 neighbors only;
- Level-2 interface: It can send and receive Level-2 packets of IS-IS protocol only, and can establish Level-2 neighbors only;
- Level-1-2 interface: It can send and receive both Level-1 and Level-2 packets of IS-IS protocol, and can establish both Level-1 and Level-2 neighbors.

IS-IS interface layer attributes relay on IS-IS global layer attributes. Level-1 intermediate system can own Level-1 interface only, Level-2 intermediate system can own Level-2 interface only, and Level-1-2 intermediate system can own all interfaces at the same time.

Table 58 Configuring Attributes of IPv6 IS-IS Global Layer

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the IS-IS configuration mode	<b>router isis [ area-tag ]</b>	-

Step	Command	Description
Configure IS-IS global layer attributes	<b>is-type</b> { <b>level-1</b>   <b>level-1-2</b>   <b>level-2-only</b> }	Optional By default, the IS-IS global layer attribute is Level-1-2.

Table 58 Configuring IS-IS Interface Layer Attributes

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure interface layer attributes	<b>isis circuit-type</b> [ <b>level-1</b>   <b>level-1-2</b>   <b>level-2</b> ]	Optional By default, when the interface layer attributes are not specified, they are consistent with global layer attributes.

### 58.2.3 Configure IPv6 IS-IS Route Generation

#### Configuration Condition

Before configuring IPv6 IS-IS route generation, ensure that:

- Configure the IPv6 address of interface so that neighbor nodes are reachable at the network layer.
- Enable the IPv6 IS-IS protocol.

#### Configure IPv6 IS-IS default route

The Level-2 area of IS-IS protocol cannot generate a default route during operation. You may add the default route information in the Level-2 LSP and send it. After this information is received by the areas of the same level of other intermediate systems, they will add a default route to the routing table.

Table 58 Configuring IS-IS Default Route

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the IS-IS configuration mode	<b>router isis [ area-tag ]</b>	-
Enter the IS-IS IPv6 address family configuration mode	<b>address-family ipv6 unicast</b>	-
Configure IS-IS to distribute default route	<b>default-information originate</b>	Mandatory By default, the default route is not advertised.

### Configure IPv6 IS-IS Route Redistribution

The routing information of other routing protocols can be imported into the IS-IS protocol through route redistribution so that the AS where IS-IS protocol is running is interconnected with the AS or routing domain where other routing protocol is running. When importing external route, you may specify the route importing policy and the layer attributes after the route is imported.

Table 58 Configuring IS-IS Route Redistribution

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the IS-IS configuration mode	<b>router isis [ area-tag ]</b>	-
Enter the IS-IS IPv6 address family configuration mode	<b>address-family ipv6 unicast</b>	-
Configure IS-IS Route Redistribution	<b>redistribute protocol [ protocol-id ] [ level-1 / level-1-2 / level-2 / metric metric-value / metric-type { external   internal } / route-map route-map-name / match route-sub-type ]</b>	Mandatory By default, the information of other routing protocol is not redistributed.

## 58.2.4 Configure IPv6 IS-IS Route Control

### Configuration Condition

Before configuring IPv6 IS-IS routing features, ensure that:

- Configure the IPv6 address of interface so that neighbor nodes are reachable at the network layer.
- Enable the IPv6 IS-IS protocol.

### Configure IPv6 IS-IS metric type

The initial IS-IS only has a narrow metric. When narrow metric is used, the maximum metric value of the interface is 63. With the gradual expansion of the network size, narrow metric is far from meeting the demand. Therefore, the metric type is expanded later to include wide metric which can reach 16777214. Devices using different metric types cannot advertise and learn routing information from each other. In order to achieve the transition between the two metric types, a configuration method for transiting metric type is provided.

Wide metric is recommended.

Table 58 Configuring IS-IS Metric Type

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the IS-IS configuration mode	<b>router isis [ area-tag ]</b>	-
Configure the metric type of interface	<b>metric-style { narrow   narrow transition   transition   wide   wide transition } [ level-1   level-1-2   level-2 ]</b>	Optional By default, narrow metric is used.

### Configure metric value of IPv6 IS-IS interface

After IS-IS protocol is enabled on the interface, the metric of IS-IS route is the global metric value, which can be separately specified for each interface through command.

Table 58 Configuring Metric Value of Interface

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Enter the IS-IS configuration mode	<b>router isis</b> [ <i>area-tag</i> ]	-
Configure IS-IS global metric value	<b>metric</b> <i>metric-value</i> [ <b>level-1</b>   <b>level-2</b> ]	Optional By default, the global metric value is 10.
Return to the global configuration mode	<b>exit</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure the metric value of interface	<b>isis ipv6 metric</b> { <i>metric-value</i> / <b>maximum</b> } [ <b>level-1</b>   <b>level-2</b> ]	Optional By default, the global metric value is used.

### Configure IPv6 IS-IS administrative distance

The system selects routes according to the administrative distance. The smaller the administrative distance, the higher the route priority.

Table 1 Configuring IS-IS Administrative Distance

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the IS-IS configuration mode	<b>router isis</b> [ <i>area-tag</i> ]	-
Enter the IS-IS IPv6 address family configuration mode	<b>address-family ipv6 unicast</b>	-
Configure the administrative distance of IS-IS route	<b>distance</b> <i>distance-value</i>	Optional By default, the administrative distance is 115.

### Configure IPv6 IS-IS route summarization

Route summarization can summarize multiple pieces of routing information into one piece of routing information. After IS-IS is configured with route summarization, it can effectively reduce the number of

subnet information reachable through advertisement, and reduce the size of the link status database and routing table, so as to effectively save memory and CPU resources. This configuration is generally used on Level-1-2 edge devices to reduce the routing information advertised between layers.

Table 2 Configuring IS-IS Route Summarization

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the IS-IS configuration mode	<b>router isis [ area-tag ]</b>	-
Enter the IPv6 address family configuration mode	<b>address-family ipv6 unicast</b>	-
Configure IS-IS Route Summarization	<b>summary-prefix prefix-value [ metric metric-value / route-type { internal   external } / metric-type { internal   external } / tag tag-value / not-advertise / level-1 / level-2 / level-1-2 ]</b>	Mandatory By default, route summarization is disabled.

### Configure the maximum number of IPv6 IS-IS load balancing entries

There may be multiple paths with the same cost that lead to the same destination address. These equal-cost paths can improve link utilization rate. Users can control the maximum number of IS-IS equal-cost routes.

Table 3 Configuring Maximum Number of IS-IS Load Balancing Entries

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the IS-IS configuration mode	<b>router isis [ area-tag ]</b>	-
Enter the IPv6 address family configuration mode	<b>address-family ipv6 unicast</b>	-

Step	Command	Description
Configure the Maximum Number of IS-IS Load Balancing Entries	<b>maximum-paths</b> <i>max-number</i>	Optional By default, the maximum number of load balancing entries is 4.

### Configure IPv6 IS-IS inter-layer route leak

By default, IS-IS only leaks Level-1 routes to Level-2, and Level-1 areas cannot know the routes in Level-2 area. You can import Level-2 routes to Level-1 by configuring inter-layer route leak. When configuring inter-layer route leak, you can specify a routing policy to only leak the route which match the conditions.

Table 4 Configuring IS-IS Inter-layer Route Leak

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the IS-IS configuration mode	<b>router isis</b> [ <i>area-tag</i> ]	-
Enter the IS-IS IPv6 address family configuration mode	<b>address-family ipv6 unicast</b>	-
Configure IS-IS Inter-area Route Leak	<b>propagate { level-1 into level-2   level-2 into level-1 } [ distribute-list <i>access-list-name</i>   route-map <i>route-map-name</i> ]</b>	Mandatory By default, Level-1 leaks routes to Level-2.

### Configure IPv6 IS-IS ATT bit

In Level-1-2 devices, ATT bit is used to advertise other nodes whether this node has connections with other areas. If yes, ATT bit will be set as 1 automatically, and other nodes will produce a default route towards this node. This will increase the business burden of this node. To change this situation, you can set ATT bit as 0.

Table 58-14 Configuring IS-IS ATT Bit

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Enter the IS-IS configuration mode	<b>router isis</b> [ <i>area-tag</i> ]	-
Enter the IS-IS IPv6 address family configuration mode	<b>address-family ipv6 unicast</b>	-
Configure IS-IS ATT Bit	<b>set-attached-bit</b> { <b>on</b>   <b>off</b> }	Mandatory By default, ATT bit is set based on whether a node has connected with other areas.

## 58.2.5 Configure IPv6 IS-IS Network Optimization

### Configuration Condition

Before configuring IPv6 IS-IS adjustment and optimization, ensure that:

- Configure the IPv6 address of interface so that neighbor nodes are reachable at the network layer.
- Enable the IPv6 IS-IS protocol.

### Configure IPv6 IS-IS interface priority

On the broadcast link, IS-IS needs to elect a node as DIS. DIS nodes send CSNP packets on a regular basis to synchronize the link status database across the network. The Level-1 and Level-2 DIS nodes are separately elected. Those with the highest interface priority are elected as DIS nodes. When the priority is the same, those with a large MAC address as DIS nodes.

Table 58 Configuring IS-IS Interface Priority

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure IS-IS Interface Priority	<b>isis priority</b> <i>priority-value</i> [ <b>level-1</b>   <b>level-2</b> ]	Optional By default, the interface priority is 64.

### Configure passive IPv6 IS-IS interface

Passive interface means the interface where no IS-IS protocol packets will be sent or received, though its direct network routing information is distributed; configuring passive IS-IS interface can save both bandwidth and the processing time of CPU; on this basis, IS-IS can also be specified to distribute direct network routing information of passive interface rather than of non-passive interface.

Table 5 Configuring Passive IS-IS Interface

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the IS-IS configuration mode	<b>router isis</b> [ <i>area-tag</i> ]	-
Configure Passive IS-IS Interface	<b>passive-interface</b> <i>interface-name</i>	Mandatory By default, there is no passive interface in IS-IS.
Configure IS-IS to distribute the routing information of passive interface only	<b>advertise-passive-only</b>	Optional By default, all the information of direct network routes that have enabled IS-IS protocol interface is distributed.

### Configure Hello packet parameters of IPv6 IS-IS

1. Configure Hello packet sending interval

After the IS-IS protocol interface is enabled, Hello packets will be periodically sent to maintain neighbor relations. The smaller the Hello packet sending interval, the larger the network convergence and the bandwidth occupied.

Table 6 Configuring Hello Packet Sending Interval

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-

Step	Command	Description
Configure Hello packet sending interval for the interface	<b>isis hello-interval</b> { <i>interval</i>   <b>minimal</b> } [ <b>level-1</b>   <b>level-2</b> ]	Optional By default, the Hello packet sending interval is 10 seconds.

### 2. Configure the number of invalid Hello packets

S-IS calculates the time of maintaining neighbor relations according to the number of invalid Hello packets, and advertise such time to neighbor devices. If the neighbor device fails to receive the Hello packets from this device during this time, it is believed the neighbor relation has become invalid, and routing calculation will be done anew.

Table 7 Configuring Number of Invalid Hello Packets

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure the number of invalid Hello packets on the interface	<b>isis hello-multiplier</b> <i>multiplier</i> [ <b>level-1</b>   <b>level-2</b> ]	Optional By default, the number of invalid Hello packets is 3.

### 3. Cancel Hello packet filling

If the MTU values of the interfaces at both ends of the link are inconsistent, large packets will not be able to pass through. To avoid this situation, IS-IS fills Hello packets to the MTU value of interface so that neighbor relation cannot be established. However, this method causes a waste of bandwidth. In actual applications, you can cancel Hello packet filling to send small Hello packets.

Table 8 Configuring Function of Cancelling Hello Packet Filling

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Cancel Hello packet filling	<b>no isis hello padding</b>	Mandatory

Step	Command	Description
		By default, the Hello packet filling function is enabled.

### Configure LSP packet parameters of IPv6 IS-IS

1. Configure the maximum Time-To-Live of LSP packets

Each LSP packet has a maximum Time-To-Live. After decreasing to zero, the Time-To-Live of LSP packets will be deleted from the link status database. The maximum Time-To-Live of LSP packets shall be greater than their refresh interval.

Table 9 Configuring Parameters of IS-IS LSP Packet

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the IS-IS configuration mode	<b>router isis [ area-tag ]</b>	-
Configure the maximum Time-To-Live of LSP packets	<b>max-lsp-lifetime</b> <i>life-time</i>	Optional By default, the maximum Time-To-Live of LSP packets is 1200 seconds.

2. Configure LSP packet refresh interval

The IS-IS protocol advertises and learns routes by interacting with their respective LSP packets. The node stores the LSP packets received in its own link state database. Each LSP packet has a maximum Time-To-Live, so all nodes need to update their LSP packets on a regular basis to prevent the maximum Time-To-Live of LSP packets from reducing to zero, and to keep the LSP packets in the entire area synchronized. Reducing the periodic LSP packet sending interval can accelerate network convergence, though it will occupy a larger bandwidth.

Table 10 Configuring LSP Packet Refresh Interval

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the IS-IS configuration mode	<b>router isis [ area-tag ]</b>	-

Step	Command	Description
Configure LSP packet refresh interval	<b>lsp-refresh-interval</b> <i>refresh-interval</i>	Optional By default, the period sending interval is 900 seconds.

### 3. Configure LSP packet generation interval

In addition to periodic update, change of interface and network status can trigger generation of new LSP packets. To avoid frequent generation of LSP packets to occupy a large amount of CPU resources, users can configure the minimum LSP packet generation interval.

Table 11 Configuring LSP Packet Generation Interval

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the IS-IS configuration mode	<b>router isis</b> [ <i>area-tag</i> ]	-
Configure LSP packet generation interval	<b>lsp-gen-interval</b> [ <i>level-1</i>   <i>level-2</i> ] <i>max-interval</i> [ <i>initial-interval</i> [ <i>secondary-interval</i> ] ]	Optional By default, the LSP packet generation interval is 50 milliseconds.

### 4. Configure LSP packet sending interval

Whenever LSP packets are generated, they are sent on the interface. To avoid frequent generation of LSP packets to occupy massive interface bandwidth, you can configure the minimum LSP packet sending interval for each interface.

Table 12 Configuring LSP Packet Sending Interval

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure LSP packet sending interval	<b>isis lsp-interval</b> <i>min-interval</i>	Optional

Step	Command	Description
		By default, the LSP packet sending interval is 33 milliseconds.

#### 5. Configure LSP packet retransmission time

On the point-to-point link, IS-IS needs to send a PSNP confirmation message from the peer port after sending LSP packet. If the confirmation message from the peer port fails to be received, the LSP packet will be resent. The time of waiting for confirmation, i.e. the LSP packet retransmission time, can be configured by users to prevent LSP packets from being retransmitted because the confirmation is not received when there is a long time delay.

Table 13 Configuring LSP Packet Retransmission Time

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure LSP packet retransmission time	<b>isis retransmit-interval</b> <i>interval [ level-1   level-2 ]</i>	Optional By default, the retransmission time is 5 seconds.

#### 6. Configure LSP MTU value

IS-IS protocol packets cannot be automatically fragmented. To ensure normal diffusion of LSP packets, the maximum length of LSP packets in a routing domain shall not exceed the minimum MTU value of the IS-IS interface of all devices; when the MTU values of the device interfaces in the routing domain are inconsistent, uniform setting of the maximum LSP packet length is recommended.

Table 14 Configuring LSP MTU Value

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the IS-IS configuration mode	<b>router isis</b> [ <i>area-tag</i> ]	-

Step	Command	Description
Configure MTU value of LSP packet	<b>lsp-mtu</b> <i>mtu-size</i> [ <b>level-1</b>   <b>level-2</b> ]	Optional By default, the MTU value of LSP packet is 1492 bytes.

### Configure SNP packet parameters of IPv6 IS-IS

#### 1. Configure CSNP packet sending interval

The broadcast link election node needs to periodically send CSNP packets to synchronize the link status database of the entire network. The periodic sending interval of CSNP packets can be adjusted based on the actual situation.

Table 15 Configuring CSNP Packet Sending Interval

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure CSNP packet sending interval	<b>isis csnp-interval</b> <i>interval</i> [ <b>level-1</b>   <b>level-2</b> ]	Optional By default, the periodic CSNP packet sending interval is 10 seconds.

#### 2. Configure PSNP packet sending interval

On the broadcast link, PSNP packets are used to synchronize the link status database of the entire network; on the point-to-point link, PSNP packets are used to confirm the received LSP packets. In order to prevent a large number of PSNP packets from being sent on the interface, a minimum sending time interval is set for PSNP packets. Users can dynamically modify this interval. A very large PSNP packet sending interval is not recommended. For broadcast links, it will affect the synchronization of the link status database of the entire network. For point-to-point links, it will cause the retransmission of LSP packets due to late receipt of confirmation.

Table 16 Configuring PSNP Packet Sending Interval

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure PSNP packet sending interval	<b>isis psnp-interval</b> <i>min-interval</i> [ <b>level-1</b>   <b>level-2</b> ]	Optional By default, the PSNP packet sending interval is 2 seconds.

### Configure SPF calculation interval of IPv6 IS-IS

The change of IS-IS link status database will trigger SPF routing calculation. Frequent SPF calculation consumes a great many CUP resources. Users may configure the SPF calculation interval.

Table 17 Configuring IS-IS SPF Calculation Interval

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the IS-IS configuration mode	<b>router isis</b> [ <i>area-tag</i> ]	-
Enter the IS-IS IPv6 address family configuration mode	<b>address-family ipv6 unicast</b>	-
Configure IS-IS SPF calculation interval	<b>spf-interval</b> [ <b>level-1</b>   <b>level-2</b> ] <i>maximum-interval</i> [ <i>min-initial-delay</i> [ <i>min-second-delay</i> ] ]	Optional By default, <i>maximum-interval</i> is 10s, <i>min-initial-delay</i> is 50ms, and <i>min-second-delay</i> is 200ms.

### Configure the maximum number of areas for IPv6 IS-IS

An IS-IS process can be configured with multiple area addresses that are mainly used for the smooth transition of merging multiple Level-1 areas into one Level-1 area, or dividing a Level-1 area into multiple Level-1 areas.

Table 18 Configuring Maximum Number of Areas for IS-IS

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Enter the IS-IS configuration mode	<b>router isis</b> [ <i>area-tag</i> ]	-
Configure the Maximum Number of IS-IS Areas	<b>max-area-addresses</b> <i>max-number</i>	Optional By default, the maximum number of area addresses is 3.

### Note

- This requires consistent configuration in the entire IS-IS Level-1 routing domain. Otherwise, Level-1 neighbors cannot be normally established. This is not the case for Level-2 neighbors.

### Configure IPv6 IS-IS host name mapping

IS-IS can uniquely identify an intermediate system through system ID. The fixed length of the system ID is 6 bytes. When viewing system information (e.g. neighbor relation, and link status database), users cannot link the system ID with host name; IS-IS supports the mapping of system ID and host name for intuitive and convenient viewing of system information by users. There are two ways to configure IS-IS host name mapping:

1. Configure IS-IS static host name mapping

IS-IS static host name mapping means the mapping that users manually establish system ID and host name for remote devices.

Table 19 Configuring IS-IS Static Host Name Mapping

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the IS-IS configuration mode	<b>router isis</b> [ <i>area-tag</i> ]	-
Configure IS-IS static host name mapping	<b>hostname static</b> <i>system-id</i> <i>host-name</i>	Mandatory

2. Configure IS-IS dynamic host name mapping

Static host name mapping requires users to configure system ID and host name mapping of other devices for each device in the network, which is a heavy workload; for dynamic host name mapping, other devices in the network can learn the host name of the device after configuring host name for each device and enabling the host name advertisement function.

Table 20 Configuring IS-IS Dynamic Host Name Mapping

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the IS-IS configuration mode	<b>router isis [ <i>area-tag</i> ]</b>	-
Configure IS-IS dynamic host name mapping	<b>hostname dynamic { <i>host-name</i>   <i>area-tag</i>   <b>recv-only</b>   <b>system-name</b> }</b>	Mandatory By default, only the host name advertised by other devices is learned.

#### Add IPv6 IS-IS interface into mesh group

Without being added into the Mesh group, the IS-IS interface will send the LSP packet received from an interface via all the other IS-IS interfaces. This causes a huge waste of bandwidth in the fully meshed network. You may add several IS-IS interfaces into the same Mesh group. After receiving the LSP packet, the interfaces only send this packet to the interfaces in other Mesh group.

Table 21 Adding IS-IS Interface into Mesh Group

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface <i>interface-name</i></b>	-
Add IS-IS Interface to Mesh Group	<b>isis mesh-group { <i>group-number</i>   <b>blocked</b> }</b>	Mandatory By default, it is not added into any Mesh group.

#### Note

- **isis mesh-group blocked** sets the interface as a blocking interface. The blocking interface

---

will not actively send LSP packets. It does so only when LSP request is received.

---

## 58.2.6 Configure IPv6 IS-IS Network Authentication

### Configuration Condition

Before configuring IPv6 IS-IS network authentication, ensure that:

- Configure the IPv6 address of interface so that neighbor nodes are reachable at the network layer.
- Enable the IPv6 IS-IS protocol.

### Configure IPv6 IS-IS neighbor authentication

After configuring IS-IS to enable neighbor relation authentication, an authentication message will be added into the Hello packet sent, and the Hello packet received will be authenticated. If the authentication fails, a neighbor relation cannot be formed. This will prevent the establishment of neighbor relation with the device which cannot be trusted.

Table 22 Configuring IS-IS Neighbor Authentication

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure Hello packet authentication mode	<b>isis authentication mode</b> { <b>md5</b>   <b>sm3</b>   <b>text</b> } [ <b>level-1</b>   <b>level-2</b> ]	Mandatory By default, the authentication function is disabled.
Configure the authentication password of Hello packet	<b>isis authentication key</b> { <b>0</b>   <b>7</b> } <i>password</i> [ <b>level-1</b>   <b>level-2</b> ]	Either-or By default, there is no authentication password; authentication password can be configured with a coding strand. For the configuration of coding strand, see the coding strand configuration section in the User Manual.
	<b>isis authentication key-chain</b> <i>key-chain-name</i> [ <b>level-1</b>   <b>level-2</b> ]	

### Configure IPv6 IS-IS route authentication

After configuring IS-IS routing information authentication, an authentication message will be added into the LSP and SNP packet, and the LSP and SNP packet received will be authenticated. If the authentication fails, the packet will be directly discarded. This will prevent the routing information which cannot be trusted from diffusing into the IS-IS network.

Table 23 Configuring IS-IS Route Authentication

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the IS-IS configuration mode	<b>router isis</b> [ <i>area-tag</i> ]	-
Configure the authentication mode of routing information packet	<b>authentication mode</b> { <b>md5</b>   <b>sm3</b>   <b>text</b> } [ <b>level-1</b>   <b>level-2</b> ]	Mandatory  By default, the authentication function is disabled.
Configure the authentication password of routing information packet	<b>authentication key</b> { <b>0</b>   <b>7</b> } <i>password</i> [ <b>level-1</b>   <b>level-2</b> ]	Either-or  By default, there is no authentication password; authentication password can be configured with a coding strand. For the configuration of coding strand, see the coding strand configuration section in the User Manual.
	<b>authentication key-chain</b> <i>key-chain-name</i> [ <b>level-1</b>   <b>level-2</b> ]	

### 58.2.7 Configure IPv6 IS-IS FRR

#### Configuration Condition

Before configuring IS-IS FRR, ensure that:

- Configure the IPv6 address of interface so that neighbor nodes are reachable at the network layer.
- Enable the IPv6 IS-IS protocol.

#### Configure IPv6 IS-IS FRR

In the IPv6 IS-IS network, as a result of link or device failure, the packets passing the point of failure will be discarded or loops will be produced. The traffic interruption caused thereby will continue until the protocol reconverges after several seconds. In order to reduce the time of traffic interruption, IS-IS FRR can be configured. By applying the routing map, set a backup next hop for the successfully matched route. Once the main link fails, the traffic passing through the failed link will immediately switch to the backup link, achieving the purpose of fast switching.

Table 24 Configuring IPv6 IS-IS FRR

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the IS-IS configuration mode	<b>router isis [ <i>area-tag</i> ]</b>	-
Enter the IS-IS IPv6 address family configuration mode	<b>address-family ipv6 unicast</b>	-
Configure IPv6 IS-IS to enable the FRR function	<b>fast-reroute route-map <i>route-map-name</i></b>	Mandatory By default, the IPv6 IS-IS FRR function is disabled.
Configure IPv6 IS-IS to enable the dynamic FRR function	<b>fast-reroute loop-free-alternate [route-map <i>route-map-name</i>]</b>	Mandatory By default, the IPv6 IS-IS dynamic FRR function is disabled.
Configure IPv6 IS-IS to enable the pic function	<b>pic</b>	Mandatory After the pic function is enabled, the auto FRR function is enabled.  By default, the IPv6 IS-IS pic function is disabled.



- 
- The IPv6 IS-IS FRR function has two types, i.e. static FRR and dynamic FRR.
  - Static FRR needs to associate route-map where the next hop interface and address of back-up route are set.
  - Currently, dynamic FRR supports point-to-point network only, i.e. all the output interfaces of the device have a network type of point-to-point. After dynamic FRR is configured, the device automatically calculates and sets back-up next hop interface and address. Dynamic FRR can also associate route-map to set back-up next hop interface and address for the route which matches the route-map only.
  - The methods of enabling rerouting are mutually exclusive;
- 

### 58.2.8 Configure IPv6 IS-IS GR

GR (Graceful Restart) is used to keep the routing information in the forwarding layer of this device and neighbor device unchanged during the switch between host and standby devices to ensure the forwarding process is not affected; after the device is switched for re-running, the two devices synchronize routing information and update forwarding layer in the protocol layer so that the data can keep forwarding during the process of device switch.

There are two types of roles in the GR process:

GR Restarter end: The device for graceful restart of protocol.

GR Helper end: The device which helps with the graceful restart of protocol.

The distributed device can act as GR Restarter and GR Helper, while the centralized device only serves as GR Helper to help the Restarter complete GR.

#### Configuration Condition

Before configuring IPv6 IS-IS GR, ensure that:

- Configure the IPv6 address of interface so that neighbor nodes are reachable at the network layer.
- Enable the IPv6 IS-IS protocol.

#### Configure IPv6 IS-IS GR Restarter

Table 25 Configuring IS-IS GR Restarter

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the IS-IS configuration mode	<b>router isis [ area-tag ]</b>	-

Step	Command	Description
Enable IS-IS to enable the GR function	<b>nsf ietf</b>	Mandatory By default, the GR function is disabled.
Configure advertisement to enter the retransmission times of GR process message	<b>nsf interface-expire</b> <i>resend-cnt</i>	Optional By default, the number of retransmission times is 3.
Configure the retransmission waiting time of GR process message	<b>nsf interface-timer</b> <i>wait-time</i>	Optional By default, the waiting time is 10 seconds.

### Configure IPv6 IS-IS GR Helper

GR Helper can help the Restarter end complete GR. By default, the device enables this function. Users can close this function via command.

Table 26 Configuring IS-IS GR Restarter

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the IS-IS configuration mode	<b>router isis</b> [ <i>area-tag</i> ]	-
Configure IS-IS GR Helper to disable the capability of Helper	<b>nsf ietf helper disable</b>	Mandatory Configure IS-IS GR Helper to disable the capability of Helper

### 58.2.9 IPv6 IS-IS monitoring and maintaining

Table 27 IPv6 IS-IS Monitoring and Maintaining

Command	Description
<b>clear isis</b> [ <b>instance -null</b>   <i>area-tag</i> ] <b>statistics</b> [ <i>interface_name</i> ]	Clear the statistical information of IPv6 IS-IS protocol operation

Command	Description
<b>clear isis [ instance -null   area-tag ] process</b>	Restart the IPv6 IS-IS protocol process
<b>show isis [ instance -null   area-tag ]</b>	Show the information of IPv6 IS-IS process
<b>show isis instance { -null   area-tag } ipv6 bfd-sessions</b>	Show the information about BFD session of IPv6 IS-IS process
<b>show isis [ instance -null   area-tag ] database [ lsp_id ] [ detail ] [ I1 / I2 ] [ level-1 / level-2 ] [ self ] [ verbose ]</b>	Show the IPv6 IS-IS link status database information
<b>show isis interface [ interface-name ] [ detail ]</b>	Show information of the interface running IPv6 IS-IS protocol
<b>show isis [ instance -null   area-tag ] ipv6 reach-info</b>	Show IPV6 subnet reachable information of IPv6 IS-IS
<b>show isis [ instance -null   area-tag ] ipv6 route</b>	Show the IPV6 routing information of IPv6 IS-IS
<b>show isis [instance -null   area-tag ] mesh-groups</b>	Show the mesh group of IPv6 IS-IS
<b>show isis [ instance -null   area-tag ] neighbors [ interface-name ] [ detail ]</b>	Show the information of IPv6 IS-IS neighbors
<b>show isis [ instance -null   area-tag ] statistics [ interface-name ]</b>	Show the statistical information of IPv6 IS-IS protocol operation
<b>show isis nsf message</b>	Show the information of IPv6 IS-IS GR
<b>show isis nsf status</b>	Show the IPv6 IS-IS GR status
<b>show isis router</b>	Show the host name information of IS-IS

## 58.3 Typical configuration example of IS-ISv6

### 58.3.1 Configure basic functions of IS-ISv6

#### Network Requirements

- Enable network interconnection between devices by configuring IS-ISv6 protocol.

- Device1 is a Level-1 router; Device2 is a Level-1-2 router; Device1 and Device2 are in the same area; the area number is 10. Device3 is a Level-2 router, and the area number is 20. Device2 connects the two areas.

## Network Topology

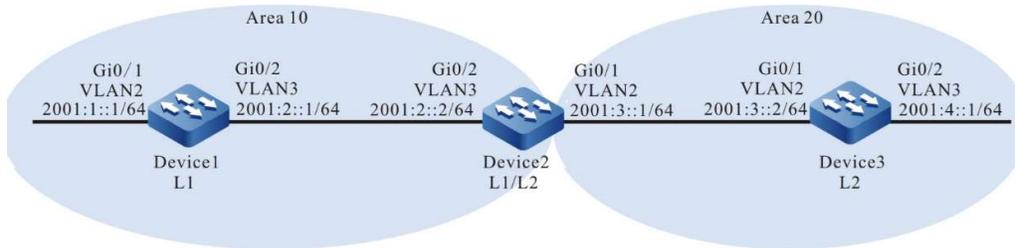


Figure 58 Network Topology for Configuring Basic Functions of IS-ISv6

## Configuration Steps

- Step 1: Configure IPv6 addresses for the ports. (Omitted)
- Step 2: Configure IS-ISv6 and enable the this process on the interface.

#On Device1, configure IS-ISv6 process 100, area number 10 and type Level-1, and enable this process on the interface.

```
Device1#configure terminal
Device1(config)#router isis 100
Device1(config-isis)#net 10.0000.0000.0001.00
Device1(config-isis)#is-type level-1
Device1(config-isis)#metric-style wide
Device1(config-isis)#address-family ipv6 unicast
Device1(config-isis-af)#multi-topology
Device1(config-isis-af)#exit-address-family
Device1(config-isis)#exit
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ipv6 router isis 100
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan3
Device1(config-if-vlan3)#ipv6 router isis 100
Device1(config-if-vlan3)#exit
```

#On Device2, configure IS-ISv6 process 100, area number 10 and type Level-1-2, and enable this process on the interface.

```
Device2#configure terminal
Device2(config)#router isis 100
Device2(config-isis)#net 10.0000.0000.0002.00
Device2(config-isis)#metric-style wide
Device2(config-isis)#address-family ipv6 unicast
Device2(config-isis-af)#multi-topology
Device2(config-isis-af)#exit-address-family
Device2(config-isis)#exit
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ipv6 router isis 100
Device2(config-if-vlan2)#exit
```

```

Device2(config)#interface vlan3
Device2(config-if-vlan3)#ipv6 router isis 100
Device2(config-if-vlan3)#exit

```

#On Device3, configure IS-ISv6 process 100, area number 20 and type Level-2, and enable this process on the interface.

```

Device3#configure terminal
Device3(config)#router isis 100
Device3(config-isis)#net 20.0000.0000.0003.00
Device3(config-isis)#is-type level-2
Device3(config-isis)#metric-style wide
Device3(config-isis)#address-family ipv6 unicast
Device3(config-isis-af)#multi-topology
Device3(config-isis-af)#exit-address-family
Device3(config-isis)#exit
Device3(config)#interface vlan2
Device3(config-if-vlan2)#ipv6 router isis 100
Device3(config-if-vlan2)#exit
Device3(config)#interface vlan3
Device3(config-if-vlan3)#ipv6 router isis 100
Device3(config-if-vlan3)#exit

```

Step 3: Check the result.

#View the information of IS-ISv6 neighbors on Device1.

```

Device1#show isis neighbors
IS-IS Instance 100 Neighbors (Counter 1):
Type System ID Interface State Holdtime Level IETF-NSF Priority Circuit ID
L1-LAN 0000.0000.0002 vlan3 Up 25 sec L1 capable 64 0000.0000.0001.02

```

#View the information of IS-ISv6 neighbors on Device2.

```

Device2#show isis neighbors
IS-IS Instance 100 Neighbors (Counter 2):
Type System ID Interface State Holdtime Level IETF-NSF Priority Circuit ID
L1-LAN 0000.0000.0001 vlan2 Up 8 sec L1 capable 64 0000.0000.0001.02
L2-LAN 0000.0000.0003 vlan3 Up 7 sec L2 capable 64 0000.0000.0003.01

```

Device2 establishes IS-ISv6 neighbors with Device1 and Device3.

#View the information of IS-ISv6 neighbors on Device 3.

```

Device3#show isis neighbors
IS-IS Instance 100 Neighbors (Counter 1):
Type System ID Interface State Holdtime Level IETF-NSF Priority Circuit ID
L2-LAN 0000.0000.0002 vlan3 Up 23 sec L2 capable 64 0000.0000.0003.01

```

#View the routing information of Device1.

```

Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
U - Per-user Static route
O - OSPF, OE-OSPF External, M - Management

i ::0 [115/10]
via fe80::201:7aff:fe5e:6d45, 00:03:17, vlan3
L ::1/128 [0/0]
via ::, 16:03:18, lo0

```

```

C 2001:1::/64 [0/0]
  via ::, 00:20:11, vlan2
L 2001:1::1/128 [0/0]
  via ::, 00:20:10, lo0
C 2001:2::/64 [0/0]
  via ::, 00:19:50, vlan3
L 2001:2::1/128 [0/0]
  via ::, 00:19:49, lo0
i 2001:3::/64 [115/20]
  via fe80::201:7aff:fe5e:6d45, 00:06:48, vlan3

Device1#show isis ipv6 route
IS-IS Instance 100, VRF Kernel, IPv6 routes table (Counter 4):
L1 ::/0, flags none, metric 10, from learned, installed
  via fe80::201:7aff:fe5e:6d45, vlan3, neighbor 0000.0000.0002
L1 2001:1::/64, flags none, metric 10, from network connected
  via ::, vlan2
L1 2001:2::/64, flags none, metric 10, from network connected
  via ::, vlan3
L1 2001:3::/64, flags none, metric 20, from learned, installed
  via fe80::201:7aff:fe5e:6d45, vlan3, neighbor 0000.0000.0002

```

There is a default route in the routing table of Device1. The next hop is Device2.

#View the routing information of Device2.

```

Device2#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
  via ::, 1d:12:42:31, lo0
i 2001:1::/64 [115/20]
  via fe80::201:7aff:fe61:7a24, 00:08:32, vlan3
C 2001:2::/64 [0/0]
  via ::, 23:41:09, vlan2
L 2001:2::2/128 [0/0]
  via ::, 23:41:06, lo0
C 2001:3::/64 [0/0]
  via ::, 17:39:09, vlan3
L 2001:3::1/128 [0/0]
  via ::, 17:39:06, lo0
i 2001:4::/64 [115/20]
  via fe80::2212:1ff:fe01:101, 00:04:52, vlan2

Device2#show isis ipv6 route
IS-IS Instance 100, VRF Kernel, IPv6 routes table (Counter 4):
L1 2001:1::/64, flags none, metric 20, from learned, installed
  via fe80::201:7aff:fe61:7a24, vlan3, neighbor 0000.0000.0001
L1 2001:2::/64, flags none, metric 10, from network connected
  via ::, vlan3
L1 2001:3::/64, flags none, metric 10, from network connected
  via ::, vlan2

```

```
L2 2001:4::/64, flags none, metric 20, from learned, installed
  via fe80::2212:1ff:fe01:101, vlan2, neighbor 0000.0000.0003
```

Device2 includes Level-1 and Level-2 routes.

#View the routing information of Device3.

```
Device3#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management
```

```
L ::1/128 [0/0]
  via ::, 00:00:12, lo0
i 2001:1::/64 [115/30]
  via fe80::201:7aff:fe5e:6d46, 00:00:12, vlan2
i 2001:2::/64 [115/20]
  via fe80::201:7aff:fe5e:6d46, 00:00:12, vlan2
C 2001:3::/64 [0/0]
  via ::, 00:00:12, vlan2
L 2001:3::2/128 [0/0]
  via ::, 00:00:12, lo0
C 2001:4::/64 [0/0]
  via ::, 00:00:12, vlan3
L 2001:4::1/128 [0/0]
  via ::, 00:00:12, lo0
```

```
Device3#show isis ipv6 route
IS-IS Instance 100, VRF Kernel, IPv6 routes table (Counter 4):
L2 2001:1::/64, flags none, metric 30, from learned, installed
  via fe80::201:7aff:fe5e:6d46, vlan2, neighbor 0000.0000.0002
L2 2001:2::/64, flags none, metric 20, from learned, installed
  via fe80::201:7aff:fe5e:6d46, vlan2, neighbor 0000.0000.0002
L2 2001:3::/64, flags none, metric 10, from network connected
  via ::, vlan2
L2 2001:4::/64, flags none, metric 10, from network connected
  via ::, vlan3
```

Device3 learns Level-1 route. By default, Level-1 leaks to Level-2.

---

## Note

- The metric type is narrow metric by default. Wide metric is recommended.
  - The IS-ISv6 entity attribute is Level-1-2 by default.
-

## 58.3.2 Configure IPv6 IS-IS static FRR

### Network Requirements

- All devices are configured with IPv6 IS-IS protocol.
- Enable static FRR between Device1 and Device3. When the lines fail, the service can quickly switch to Device2 for communication.

### Network Topology

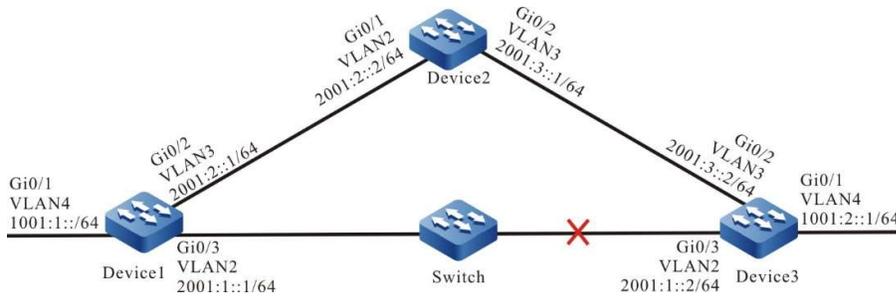


Figure 58 Network Topology for Configuring IPv6 IS-IS Static FRR

### Configuration Steps

Step 1: Configure VLAN, and add ports to the required VLAN; configure the IPv6 address of each interface. (Omitted)

Step 2: Configure IS-ISv6 and enable the this process on the interface.

#On Device1, configure IS-ISv6 process 100, area number 10 and type Level-2, and enable this process on the interface.

```
Device1#configure terminal
Device1(config)#router isis 100
Device1(config-isis)#net 10.0000.0000.0001.00
Device1(config-isis)#is-type level-2
Device1(config-isis)#metric-style wide
Device1(config-isis)#exit
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ipv6 router isis 100
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan3
Device1(config-if-vlan3)#ipv6 router isis 100
Device1(config-if-vlan3)#exit
```

#On Device2, configure IS-ISv6 process 100, area number 10 and type Level-2, and enable this process on the interface.

```
Device2#configure terminal
Device2(config)#router isis 100
Device2(config-isis)#net 10.0000.0000.0002.00
Device2(config-isis)#is-type level-2
Device2(config-isis)#metric-style wide
Device2(config-isis)#exit
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ipv6 router isis 100
Device2(config-if-vlan2)#exit
```

```

Device2(config)#interface vlan3
Device2(config-if-vlan3)#ipv6 router isis 100
Device2(config-if-vlan3)#exit

```

#On Device3, configure IS-ISv6 process 100, area number 10 and type Level-2, and enable this process on the interface.

```

Device3#configure terminal
Device3(config)#router isis 100
Device3(config-isis)#net 10.0000.0000.0003.00
Device3(config-isis)#is-type level-2
Device3(config-isis)#metric-style wide
Device3(config-isis)#exit
Device3(config)#interface vlan2
Device3(config-if-vlan2)#ipv6 router isis 100
Device3(config-if-vlan2)#exit
Device3(config)#interface vlan3
Device3(config-if-vlan3)#ipv6 router isis 100
Device3(config-if-vlan3)#exit
Device3(config-if-vlan4)#ipv6 router isis 100
Device3(config-if-vlan4)#exit

```

#### Step 4: Configure routing policy.

#On Device1, configure route-map to invoke ACL to match 1001:2::1/64 only, and filter other network segments. The route matching the match rule applies the backup next hop interface vlan3. The next hop address is 2001:2::2.

```

Device1(config)#ipv6 access-list extended 7001
Device1(config-v6-list)#permit ipv6 1001:2::1/64 any
Device1(config-v6-list)#exit
Device1(config)#route-map ipv6frr_isis
Device1(config-route-map)#match ipv6 address 7001
Device1(config-route-map)#set ipv6 fast-reroute backup-interface vlan2 backup-next-hop 2001:2::2
Device1(config-route-map)#exit

```

#### Step 5: Configure static FRR.

```

Device1(config)#router isis 100
Device1(config-isis)#address-family ipv6 unicast
Device1(config-isis-af)#fast-reroute route-map ipv6frr_isis
Device1(config-isis-af)#exit-address-family
Device1(config-isis)#exit

```

#### Step 6: Check the results.

#View IPv6 IS-IS routing table on Device1.

```

Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management
L ::1/128 [0/0]
  via ::, 06:22:27, lo0
C 1001:1::/64 [0/0]
  via ::, 06:17:34, vlan4
L 1001:1::1/128 [0/0]
  via ::, 06:17:34, vlan4
i 1001:2::/64 [115/20]
  via fe80::201:7aff:fe92:e6b6, 00:10:32, vlan2
C 2001:1::/64 [0/0]
  via ::, 01:24:08, vlan2
L 2001:1::1/128 [0/0]
  via ::, 01:24:08, vlan2

```

```

C 2001:2::/64 [0/0]
  via ::, 06:16:52, vlan3
L 2001:2::1/128 [0/0]
  via ::, 06:16:52, vlan3
i 2001:3::/64 [115/20]
  via fe80::201:7aff:fe92:e6b6, 00:29:05, vlan2
  via fe80::ced8:1fff:fe10:7aae, 00:35:19, vlan3

```

According to the routing table, the route 1001:2::/64 prefers the lines between Device1 and Device3 for communication.

#View IPv6 FRR routing table on Device1.

```

Device1#show ipv6 frr route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management
i 1001:2::/64 [115/4294967295]
  via 2001:2::2, 00:13:16, vlan3

```

According to the result, the next hop and output interface of the frr route 1001:2::/64 are 2001:2::2 and vlan3 respectively.

#View the BFD session information of Device1.

```

Device1#show bfd session ipv6 2001:1::1 detail
Total ipv6 session number: 1
OurAddr      NeighAddr      LD/RD      State  Holddown  Interface
2001:1::1    2001:1::1      1012/1012  UP     500       vlan2
Type:ipv6 direct Mode:echo
Local Discriminator:301 Remote Discriminator:301
Local State:UP Remote State:UP Up for: 0h:15m:38s Number of times UP:1
Send Interval:100ms Detection time:500ms(100ms*5)
Local Diag:0 Demand mode:0 Poll bit:0
Registered modules:FIB_MGR

```

According to the result, FIB\_MGR has been successfully coordinated with BFD. The session is established normally in the mode of echo.

#When the lines between Device1 and Device3 fail, it can quickly identify the failures and switch to Device2 for communication. The routing table of Device1 shows that the output interface of the destination network 1001:2::/64 has switched to the backup interface vlan3.

```

Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management
L ::1/128 [0/0]
  via ::, 06:29:08, lo0
C 1001:1::/64 [0/0]
  via ::, 06:24:15, vlan4
L 1001:1::1/128 [0/0]
  via ::, 06:24:15, vlan4
i 1001:2::/64 [115/30]
  via fe80::ced8:1fff:fe10:7aae, 00:00:01, vlan3
i 2001:1::/64 [115/30]
  via fe80::ced8:1fff:fe10:7aae, 00:00:01, vlan3
C 2001:2::/64 [0/0]
  via ::, 06:23:33, vlan3
L 2001:2::1/128 [0/0]
  via ::, 06:23:33, vlan3
i 2001:3::/64 [115/20]
  via fe80::ced8:1fff:fe10:7aae, 00:42:00, vlan3

```

### 58.3.3 Configure IPv6 IS-IS dynamic FRR

#### Network Requirements

- All devices are configured with IPv6 IS-IS protocol.
- Enable dynamic FRR between Device1 and Device3. When the lines fail, the service can quickly switch to Device2 for communication.

#### Network Topology

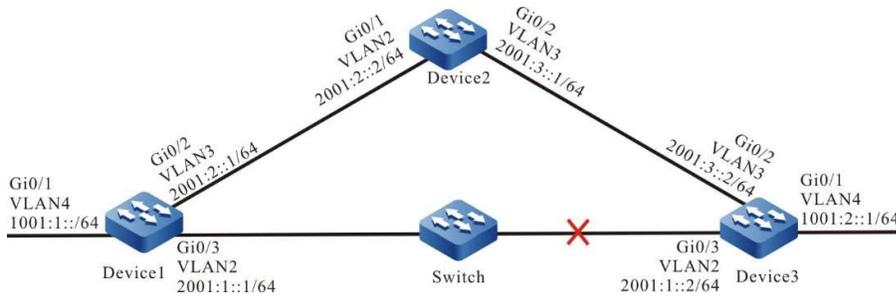


Figure 1 Network Topology for Configuring IPv6 IS-IS Dynamic FRR

#### Configuration Steps

Step 1: Configure VLAN, and add ports to the required VLAN; configure the IPv6 address of each interface. (Omitted)

Step 2: Configure IS-ISv6 and enable the this process on the interface.

#On Device1, configure IS-ISv6 process 100, area number 10 and type Level-2, and enable this process on the interface. Configure the network type of the interface as point-to-point.

```
Device1#configure terminal
Device1(config)#router isis 100
Device1(config-isis)#net 10.0000.0000.0001.00
Device1(config-isis)#is-type level-2
Device1(config-isis)#metric-style wide
Device1(config-isis)#exit
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ipv6 router isis 100
Device1(config-if-vlan2)# isis network point-to-point
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan3
Device1(config-if-vlan3)#ipv6 router isis 100
Device1(config-if-vlan3)# isis network point-to-point
Device1(config-if-vlan3)#exit
```

#On Device2, configure IS-ISv6 process 100, area number 10 and type Level-2, and enable this process on the interface. Configure the network type of the interface as point-to-point.

```
Device2#configure terminal
Device2(config)#router isis 100
Device2(config-isis)#net 10.0000.0000.0002.00
Device2(config-isis)#is-type level-2
Device2(config-isis)#metric-style wide
Device2(config-isis)#exit
Device2(config)#interface vlan2
```

```

Device2(config-if-vlan2)#ipv6 router isis 100
Device2(config-if-vlan2)# isis network point-to-point
Device2(config-if-vlan2)#exit
Device2(config)#interface vlan3
Device2(config-if-vlan3)#ipv6 router isis 100
Device2(config-if-vlan3)# isis network point-to-point
Device2(config-if-vlan3)#exit

```

#On Device3, configure IS-ISv6 process 100, area number 10 and type Level-2, and enable this process on the interface. Configure the network type of the interface as point-to-point.

```

Device3#configure terminal
Device3(config)#router isis 100
Device3(config-isis)#net 10.0000.0000.0003.00
Device3(config-isis)#is-type level-2
Device3(config-isis)#metric-style wide
Device3(config-isis)#exit
Device3(config)#interface vlan2
Device3(config-if-vlan2)#ipv6 router isis 100
Device3(config-if-vlan2)# isis network point-to-point
Device3(config-if-vlan2)#exit
Device3(config)#interface vlan3
Device3(config-if-vlan3)#ipv6 router isis 100
Device3(config-if-vlan3)# isis network point-to-point
Device3(config-if-vlan3)#exit
Device3(config-if-vlan4)#ipv6 router isis 100
Device3(config-if-vlan4)# isis network point-to-point
Device3(config-if-vlan4)#exit

```

### Step 3: Configure routing policy.

#On Device1, configure route-map to invoke ACL to match 1001:2::1/64 only, and filter other network segments.

```

Device1(config)#ipv6 access-list extended 7001
Device1(config-v6-list)#permit ipv6 1001:2::1/64 any
Device1(config-v6-list)#exit
Device1(config)#route-map ipv6frr_isis
Device1(config-route-map)#match ipv6 address 7001
Device1(config-route-map)#exit

```

### Step 4: Configure static FRR.

```

Device1(config)#router isis 100
Device1(config-isis)#address-family ipv6 unicast
Device1(config-isis-af)# fast-reroute loop-free-alternate route-map ipv6frr_isis
Device1(config-isis-af)#exit-address-family
Device1(config-isis)#exit

```

### Step 5: Check the results.

#View IPv6 IS-IS routing table on Device1.

```

Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management
L ::1/128 [0/0]
  via ::, 06:22:27, lo0
C 1001:1::/64 [0/0]
  via ::, 06:17:34, vlan4
L 1001:1::1/128 [0/0]
  via ::, 06:17:34, vlan4
i 1001:2::/64 [115/20]
  via fe80::201:7aff:fe92:e6b6, 00:10:32, vlan2

```

```

C 2001:1::/64 [0/0]
  via ::, 01:24:08, vlan2
L 2001:1::1/128 [0/0]
  via ::, 01:24:08, vlan2
C 2001:2::/64 [0/0]
  via ::, 06:16:52, vlan3
L 2001:2::1/128 [0/0]
  via ::, 06:16:52, vlan3
i 2001:3::/64 [115/20]
  via fe80::201:7aff:fe92:e6b6, 00:29:05, vlan2
  via fe80::ced8:1fff:fe10:7aae, 00:35:19, vlan3

```

According to the routing table, the route 1001:2::/64 prefers the lines between Device1 and Device3 for communication.

#### #View IPv6 FRR routing table on Device1.

```

Device1#show ipv6 frr route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management
i 1001:2::/64 [115/4294967295]
  via fe80::ced8:1fff:fe10:7aae, 00:07:18, vlan3

```

#### #View the BFD session information of Device1.

```

Device1#show bfd session ipv6 2001 :1 ::1 detail
Total ipv6 session number: 1
OurAddr      NeighAddr      LD/RD      State      Holddown  Interface
2001 :1 ::1  2001 :1 ::1    1012/1012  UP         500      vlan2
Type:ipv6 direct Mode:echo
Local Discriminator:301 Remote Discriminator:301
Local State:UP Remote State:UP Up for: 0h:15m:38s Number of times UP:1
Send Interval:100ms Detection time:500ms(100ms*5)
Local Diag:0 Demand mode:0 Poll bit:0
Registered modules:FIB_MGR

```

According to the result, FIB\_MGR has been successfully coordinated with BFD. The session is established normally in the mode of echo.

#When the lines between Device1 and Device3 fail, it can quickly identify the failures and switch to Device2 for communication. The routing table of Device1 shows that the output interface of the destination network 1001:2::/64 has switched to the backup interface vlan3.

```

Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management
L ::1/128 [0/0]
  via ::, 06:29:08, lo0
C 1001:1::/64 [0/0]
  via ::, 06:24:15, vlan4
L 1001:1::1/128 [0/0]
  via ::, 06:24:15, vlan4
i 1001:2::/64 [115/30]
  via fe80::ced8:1fff:fe10:7aae, 00:00:01, vlan3
i 2001:1::/64 [115/30]
  via fe80::ced8:1fff:fe10:7aae, 00:00:01, vlan3
C 2001:2::/64 [0/0]
  via ::, 06:23:33, vlan3
L 2001:2::1/128 [0/0]
  via ::, 06:23:33, vlan3
i 2001:3::/64 [115/20]
  via fe80::ced8:1fff:fe10:7aae, 00:42:00, vlan3

```

# 59 IRMP

---

## 59.1 Overview

IRMP (Internal Routing Message Protocol), compatible with Cisco's EIGRP, is a dynamic routing protocol based on distance vector. IRMP uses the diffusing update algorithm for parallel computing between multiple devices to ensure zero loop and fast convergence. While overcoming the defect of slow convergence of distance vector routing protocol, it needs no link status routing protocol to run the Dijkstra algorithm, and can avoid the huge consumption of CPU and memory by relevant database.

IRMP is applicable to small and medium-sized networks. It supports multiple AS that are independent of each other.

## 59.2 IRMP function configuration

Table 59 IRMP Function Configuration List

Configuration Task	
Configure Basic Functions of IRMP	Enable IRMP Protocol
Configure IRMP Route Generation	Configure IRMP Route Redistribution
Configure IRMP Route Control	Configure IRMP Route Summarization
	Configure IRMP Administrative Distance
	Configure IRMP Load Balancing
	Configure IRMP Route Filtration

Configuration Task	
	Configure IRMP Metric Offset
	Configure Metric Value of IRMP Route
Configure IRMP Network Optimization	Configure Passive IRMP Interface
	Configure IRMP Stub
	Configure IRMP Intelligent Query
	Configure IRMP Split Horizon
	Configure IRMP Timer
	Configure IRMP Static Neighbors
Configure IRMP Network Authentication	Configure IRMP Authentication

### 59.2.1 Configure Basic Functions of IRMP

In the various configuration tasks of IRMP, you must first enable the IRMP protocol so that the configuration of the other function features can take effect.

#### Configuration Condition

Before configuring the basic functions of IRMP, do the following:

- The link layer protocol has been configured to ensure normal communication at the link layer.
- Interface IP addresses have been configured so that neighbor nodes are reachable at the network layer.

#### Enable IRMP Protocol

To use IRMP, the following configurations are required:

- Create IRMP process;
- Configure the direct network segment covered by IRMP.

Table 59 Enabling IRMP Protocol

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Create IRMP process and enter IRMP configuration mode	<b>router irmp</b> <i>autonomous-system-number</i>	Mandatory By default, IRMP process is disabled.
Configure the direct network segment covered by IRMP	<b>network</b> <i>ip-address</i> [ <i>wildcard-mask</i> ]	Mandatory By default, no direct network segment is covered.  When no inverse mask is carried, it is classful network address by default.

---

### Note

- When establishing IRMP neighbors, ensure the AS number is consistent. Otherwise, neighbor relation cannot be established.
- 

## 59.2.2 Configure IRMP Route Generation

In IRMP, cover the routes in direct network segment via the command **network**, and import external routes through redistribution.

### Configuration Condition

Before configuring IRMP route generation, ensure that:

- Interface IP addresses have been configured so that neighbor nodes are reachable at the network layer;
- Enable IRMP protocol.

### Configure IRMP Route Redistribution

The routes generated by other protocols can be imported into IRMP by configuring route redistribution. The routes of other IRMP processes can also be imported.

Table 59 Configuring IRMP Route Redistribution

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the IRMP configuration mode	<b>router irmp</b> <i>autonomous-system-number</i>	-
Configure IRMP Route Redistribution	<b>redistribute protocol</b> [ <i>process-id</i> ] [ <b>route-map</b> <i>route-map-name</i> / <b>metric</b> <i>bandwidth delay reliability loading mtu</i> ]	Mandatory By default, external routes are not redistributed.
Configure IRMP to redistribute the default metric value of external route	<b>default-metric</b> <i>bandwidth delay reliability loading mtu</i>	Optional

---

### Note

- When **default-metric** and **redistribute protocol** [ *process-id* ] **metric** are both configured, the latter has a higher priority.
- 

## 59.2.3 Configure IRMP Route Control

### Configuration Condition

Before configuring IRMP route control, ensure that:

- Interface IP addresses have been configured so that neighbor nodes are reachable at the network layer;
- Enable IRMP protocol.

### Configure IRMP Route Summarization

Both the IRMP summarized route and the original detail route appear in the local routing table. In large and medium-sized networks, only advertising the summarized route to neighbor can significantly decrease the size of the neighbor's routing table, and reduce the consumption of network bandwidth by protocol packets.

IRMP supports automatic summarization and interface address summarization. The metric value of the summarized route uses the minimum metric value among all detail routes.

## 1. Automatic summarization

For automatic summarization, the route is summarized into corresponding classful network address under non- manual configuration by users. Automatic summarization is applicable to the routes in direct network segment only.

Table 59 Configuring IRMP Automatic Summarization

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the IRMP configuration mode	<b>router irmp</b> <i>autonomous-system-number</i>	-
Configure IRMP automatic summarization	<b>auto-summary</b>	Optional By default, the IRMP automatic summarization function is disabled.

## 2. Interface address summarization

For interface address summarization, a pair of destination address and mask combination needs to be configured. They will summarize the routes covered by this network segment.

Table 59 Configuring IRMP Interface Address Summarization

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure IRMP interface address summarization	<b>ip summary-address irmp</b> <i>autonomous-system-number ip-address mask</i>	Mandatory

---

### Note

- For automatic summarization, only the routes in the direct network segment are summarized, and it will result in the reestablishment of all neighbors in the process.
- Interface route summarization is applicable to all the IRMP routes from the specified

---

interface. It will result in the reestablishment of all neighbors on the specified interface.

- Interface route summarization precedes automatic summarization.
  - Interface route summarizations are independent of each other. That is to say, when interface summarizations of 10.1.0.0/16 and 10.0.0.0/8 are configured, IRMP will advertise the two summarized routes at the same time.
- 

### Configure IRMP Administrative Distance

Administrative distance is used to make routing decisions for the same network segment routes from different protocols, and routes with a small administrative distance take precedence. Routing decisions can be affected by modifying the administrative distance of IRMP routes.

Table 59 Configuring IRMP Administrative Distance

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the IRMP configuration mode	<b>router irmp</b> autonomous-system-number	-
Configure IRMP Administrative Distance	<b>distance { irmp</b> <i>internal-routes-distance</i> <i>external-routes-distance</i>   <b>summary</b> <i>summary-routes-distance</i> }	Optional  By default, the administrative distance of internal routes of IRMP is 90, and that of external routes is 170. The summarized route has an administrative distance of 5.

---

### Note

- Configuring IRMP administrative distance will result in the reestablishment of all neighbors in the process.
- 

### Configure IRMP Load Balancing

IRMP supports equal-cost load balancing and unequal-cost load balancing. When there are multiple routes with the same metric leading to a certain destination network, equal-cost load balancing can be formed;

when there are multiple routes with different metrics leading to a certain destination network, the transformation factor can be modified through the command **variance** to form unequal-cost load balancing.

Variance defines a transformation factor to identify the action scope of unequal-cost load balancing routes. When the metric value of a non-optimal route is less than the metric value of the optimal route multiplied by the variance value, the route is selected as an unequal-cost load balancing route.

The **maximum-paths** command is used to control the maximum number of load balancing entries of IRMP. It supports 32 loads at most. When the *path-number* is configured as 1, the load function is cancelled. The IRMP load balancing entries include both equal-cost load and unequal-cost load. IRMP selects the paths that can be used as load balancing according to the transformation factor variance.

Table 59 Configuring IRMP Load Balancing

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the IRMP configuration mode	<b>router irmp</b> <i>autonomous-system-number</i>	-
Configure IRMP transformation factor to form unequal-cost load	<b>variance</b> <i>number</i>	Optional By default, the value of transformation factor is 1.
Configure the Maximum Number of IRMP Load Balancing Entries	<b>maximum-paths</b> <i>path-number</i>	Optional By default, IRMP supports up to 4 load balancing entries.

### Configure IRMP Route Filtration

Control the routes received or sent by configuring ACLs or prefix lists, and configure route filtration in the in and out directions on the interface at the same time.

Table 59 Configuring IRMP Route Filtration

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Enter the IRMP configuration mode	<b>router irmp</b> <i>autonomous-system-number</i>	-
Configure IRMP Route Filtration	<b>distribute-list</b> { <i>access-list-name</i>   <b>gateway</b> <i>prefix-list-name1</i>   <b>prefix</b> <i>prefix-list-name2</i> [ <b>gateway</b> <i>prefix-list-name3</i> ] } { <b>in</b>   <b>out</b> } [ <i>interface-name</i> ]	Mandatory

## Note

- IRMP route filtration supports standard ACL only.
- Filtration can be configured on all the interfaces, or on some interfaces through the parameter *interface-name*. When it is configured simultaneously, they are permitted to pass only when both of the two filtering rules are permitted.

### Configure IRMP Metric Offset

By default, IRMP route applies the metric value advertised by the neighbor. To modify the metric value in some special application scenarios, users can configure the IRMP metric offset to correct the metric value of the specified route.

When the metric offset in the incoming direction is configured, the routing metric value is modified when receiving the IRMP route, saved in the routing table, and advertised to neighbors. When the metric offset in the outgoing direction is configured, only the metric value advertised to the neighbor route is modified, with the local one remaining unchanged.

Table 59 Configuring IRMP Metric Offset

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the IRMP configuration mode	<b>router irmp</b> <i>autonomous-system-number</i>	-

Step	Command	Description
Configure IRMP Metric Offset	<b>offset-list</b> <i>access-list-name</i> { <b>in</b>   <b>out</b> } <i>offset-value</i> [ <i>interface-name</i> ]	Mandatory

## Note

- IRMP metric offset supports standard ACL only.
- Configuring IRMP metric offset will result in the reestablishment of all neighbors in the process.

### Configure Metric Value of IRMP Route

IRMP calculates a composite metric value as the routing metric value based on the link characteristics, including bandwidth, time delay, load, and reliability. Calculation method: Routing metric =  $256 * \left( \frac{k1 * (10^7 / \text{bandwidth}) + k2 * (10^7 / \text{bandwidth}) / (256 - \text{load}) + k3 * (\text{time delay} / 10) * [k5 / (\text{reliability} + k4)] \right)$ . Of which, the bandwidth unit is Kbit/s, the time delay unit is microsecond, and each k value denotes the weighted value of corresponding link characteristic. By default, IRMP selects link width and time delay as metric values.

Table 59 Configuring IRMP Routing Metric Value

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the IRMP configuration mode	<b>router irmp</b> <i>autonomous-system-number</i>	-
Configure IRMP Routing Metric Value	<b>metric weights</b> <i>tos k1 k2 k3 k4 k5</i>	Mandatory  tos means service type. Only 0-type service is supported.  By default, $k1=k3=1$ , $k2=k4=k5=0$ . When establishing neighbors, the k value must be consistent. Otherwise, neighbor

Step	Command	Description
		relation cannot be established.

## 59.2.4 Configure IRMP Network Optimization

### Configuration Condition

Before configuring IRMP network optimization, ensure that:

- Interface IP addresses have been configured so that neighbor nodes are reachable at the network layer;
- Enable IRMP protocol.

### Configure Passive IRMP Interface

Dynamic routing protocol uses passive interface, which can effectively reduce the consumption of network bandwidth by routing protocol. In IRMP, configuring passive interface can suppress the sending and receiving of IRMP packets on the specified interface. For example, after vlan2 is configured as a passive interface, even if the network segment where this interface is located is covered through the command **network**, IRMP will not receive or send packets on this interface.

Table 1 Configuring Passive IRMP Interface

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the IRMP configuration mode	<b>router irmp</b> <i>autonomous-system-number</i>	-
Configure Passive IRMP Interface	<b>passive interface</b> <i>interface-name</i>	Mandatory

### Configure IRMP Stub

IRMP Stub can effectively improve IRMP network stability and reduce occupation of resources. The Stub function is usually used in the hub and spoke network topology. To enable this function, users simply need to configure Stub on the spoke router. It's unnecessary to change configuration on the hub router. The spoke router specifies the type of route to be advertised through the **irmp stub** command, and the hub router will not send query packets to Stub neighbors.

Table 2 Configuring IRMP Stub

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the IRMP configuration mode	<b>router irmp</b> <i>autonomous-system-number</i>	-
Configure IRMP Stub	<b>irmp stub</b> { <b>receive-only</b> }   { <b>connected</b> / <b>summary</b> / <b>redistributed</b> }	Mandatory By default, the Stub mode is disabled.

### Note

- Modifying Stub configuration will result in the reestablishment of all neighbors in the process.

### Configure IRMP Intelligent Query

Configuring IRMP intelligent query to control the sending of query packets can effectively cut down packet interactions in the network so as to reduce resource occupation. When the intelligent query function is enabled, the device will not send query packets to the neighbors with routes cancelled to reduce the number of query and response packets in the network.

Table 3 Configuring IRMP Stub

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the IRMP configuration mode	<b>router irmp</b> <i>autonomous-system-number</i>	-
Configure IRMP intelligent query	<b>smart-query infinity-update</b>	Mandatory By default, intelligent query is disabled.

### Configure IRMP Split Horizon

IRMP split horizon means that the route learnt from an interface by IRMP will not be advertised from this interface to prevent loops from being produced.

Table 4 Configuring IRMP Split Horizon

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure IRMP split horizon	<b>ip split-horizon irmp</b> <i>autonomous-system-number</i>	Optional By default, the split horizon function is enabled.

### Configure IRMP Timer

#### 1. Configure Keepalive Timer of IRMP Neighbors

IRMP Hello packets are used to identify and keep alive neighbors. They are diffused through periodic unreliable multicast (multicast address 224.0.0.10) on the network. The default sending interval of Hello packets is determined by the network type of the sending interface: 5 seconds on broadcast and point-to-point interface, and 60 seconds on NBMA interface.

Hold time means the invalid time interval of IRMP neighbors. When a device receives a Hello packet from its neighbor, this packet will contain a hold time which tells this device the maximum valid time of the neighbor; if the Hello packet is not received from the neighbor within this time, it is deemed that the neighbor is unreachable and it will be deleted. By default, hold time is 3 times the Hello interval.

Table 5 Configuring Keepalive Timer of IRMP Neighbor

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure IRMP Hello interval	<b>ip hello-interval irmp</b> <i>autonomous-system hello-time</i>	Optional By default, Hello interval is 5 seconds or 60 seconds depending on the network type.

Step	Command	Description
Configure IRMP hold time	<b>ip hold-time irmp</b> <i>autonomous-system-number hold-time</i>	Optional By default, hold time is 3 times the Hello interval.

## 2. Configure Keepalive Timer of IRMP Routes

IRMP uses DUAL (Diffusing Update Algorithm) to learn routes. When the diffusion calculation begins, an Active-timer is started. If the response to all query packets is not received after time out, the neighbors that give no response will be deleted from the neighbor list, and the route that receives no response is set as Active and considered unreachable.

When IRMP receives a neighbor request, if the local route is also learnt from other neighbors, it will not give a response immediately. Instead, it will start a Hold Down timer and wait for a period of time. During this period of time, if no request packet is received from the neighbor, a response packet will be given to prevent loops from being produced.

Table 6 Configuring IRMP Route Timer

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the IRMP configuration mode	<b>router irmp</b> <i>autonomous-system-number</i>	-
Configure the timeout time of Active-timer	<b>timers active-time</b> <i>minutes</i>	Optional The default timeout time of Active-timer is 3 minutes.
Configure the timeout time of hold down	<b>timers holddown-time</b> <i>seconds</i>	Optional By default, the timeout time of hold down is 5 seconds.

### Note

- Configuring route timer will result in the reestablishment of all neighbors in the process.

## Configure IRMP Static Neighbors

Configure IRMP static neighbors to enable all IRMP packets between neighbors interact with each other in unicast manner.

To run the IRMP dynamic routing protocol on NBMA network which doesn't support broadcast (e.g. X.25, Frame), you can configure static neighbors. This should be done in pairs on both sides, otherwise neighbor relation cannot be established.

Table 7 Configuring IRMP Static Neighbors

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the IRMP configuration mode	<b>router irmp</b> <i>autonomous-system-number</i>	-
Configure IRMP Static Neighbors	<b>neighbor</b> <i>neighbor-ip-address interface-name</i>	Mandatory

## 59.2.5 Configure IRMP Network Authentication

### Configuration Condition

Before configuring IRMP authentication, ensure that:

- Interface IP addresses have been configured so that neighbor nodes are reachable at the network layer;
- Enable IRMP protocol.

### Configure IRMP Authentication

Check and verify the effectiveness of IRMP packets by configuring IRMP authentication to improve network security. IRMP supports MD5 authentication only.

Table 8 Configuring IRMP Authentication

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-

Step	Command	Description
Configure IRMP authentication function	<b>ip message-digest-key irmp</b> <i>autonomous-system-number</i> <i>key-id md5 { 0   7 }</i> <i>password</i>	Mandatory

## Note

- To establish IRMP neighbor relation, you need to configure the same Key-id and password on the interface.

## 59.2.6 IRMP monitoring and maintaining

Table 9 IRMP Monitoring and Maintaining

Command	Description
<b>clear ip irmp error</b>	Clear statistics of IGMP error packets
<b>clear ip irmp</b> [ <i>autonomous-system-number</i> ] <b>neighbors</b> [ <i>interface-name</i> ]	Reset IRMP neighbors
<b>clear ip irmp traffic</b> [ <i>autonomous-system-number</i> ]	Clear statistics of sending and receiving IRMP packets
<b>show ip irmp error</b>	Show statistics of IGMP error packets
<b>show ip irmp interface</b> [ <i>autonomous-system-number</i> ]   [ <i>interface-name</i> ]	Show IRMP interface information
<b>show ip irmp neighbor</b> [ <i>autonomous-system-number</i>   <b>detail</b>   <i>interface-name</i> ]	Show IRMP neighbor information
<b>show ip irmp topology</b> [ <i>autonomous-system-number</i> ] [ <b>active</b>   <b>detail</b>   <b>summary</b>   <i>ip-address mask</i> ]	Show the routing information in the IRMP topology table
<b>show ip irmp traffic</b> [ <i>autonomous-system-number</i> ]	Show statistics of sending and receiving IRMP packets

## 59.3 Typical configuration example of IRMP

### 59.3.1 Configure Basic Functions of IRMP

#### Network Requirements

- Run IRMP between Device1 and Device2 for establishment of neighbors and route interaction.

#### Network Topology

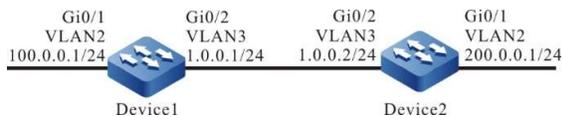


Figure 59 Network Topology for Basic Functions of IRMP

#### Configuration Steps

Step 1: Configure IP addresses for the ports. (Omitted)

Step 2: Configure IRMP.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#router irmp 100
Device1(config-irmp)#network 1.0.0.0 0.0.0.255
Device1(config-irmp)#network 100.0.0.0 0.0.0.255
Device1(config-irmp)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#router irmp 100
Device2(config-irmp)#network 1.0.0.0 0.0.0.255
Device2(config-irmp)#network 200.0.0.0 0.0.0.255
Device2(config-irmp)#exit
```

Step 3: Check the result.

#View the information of IRMP neighbors on Device1.

```
Device1#show ip irmp neighbor
IP-IRMP neighbors for process 100 Total neighbor 1
Address      Interface      Hold(s)  Uptime    SeqNum  Srtt(ms)  Rto(s)
1.0.0.2      vlan3          11       00:01:19  1        16         2
```

#View the information of IRMP neighbors on Device2.

```
Device2#show ip irmp neighbor
IP-IRMP neighbors for process 100 Total neighbor 1
Address      Interface      Hold(s)  Uptime    SeqNum  Srtt(ms)  Rto(s)
1.0.0.1      vlan3          11       00:01:19  1        16         2
```

According to the result, IRMP neighbor has been successfully established between Device1 and Device2.

#View topology table and routing table on Device1.

```
Device1#show ip irmp topology
IP-IRMP Topology Table for process 100
Codes: P - Passive, A - Active, H - Holddown, D - Hidden
> - FIB route, * - FIB successor

P >1.0.0.0/24, 1 successors, FD is 28160
   *via Connected (28160/0), vlan3
P >200.0.0.0/24, 1 successors, FD is 30720
   *via 1.0.0.2 (30720/28160), vlan3
P >100.0.0.0/24, 1 successors, FD is 28160
   *via Connected (28160/0), vlan2

Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 1.0.0.0/24 is directly connected, 00:27:02, vlan3
E 200.0.0.0/24 [90/30720] via 1.0.0.2, 00:15:07, vlan3
C 100.0.0.0/24 is directly connected, 00:27:14, vlan2
C 127.0.0.0/8 is directly connected, 137:46:13, lo0
```

Device1 learns the route 200.0.0.0/24 advertised by Device2.

#View the IRMP topology table and routing table of Device2.

```
Device2#show ip irmp topology
IP-IRMP Topology Table for process 100
Codes: P - Passive, A - Active, H - Holddown, D - Hidden
> - FIB route, * - FIB successor

P >1.0.0.0/24, 1 successors, FD is 28160
   *via Connected (28160/0), vlan3
P >200.0.0.0/24, 1 successors, FD is 28160
   *via Connected (28160/0), vlan2
P >100.0.0.0/24, 1 successors, FD is 30720
   *via 1.0.0.1 (30720/28160), vlan3

Device2#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 1.0.0.0/24 is directly connected, 00:20:12, vlan3
C 200.0.0.0/24 is directly connected, 00:19:53, vlan2
E 100.0.0.0/24 [90/30720] via 1.0.0.1, 00:08:41, vlan3
C 127.0.0.0/8 is directly connected, 361:04:08, lo0
```

Device2 learns the route 100.0.0.0/24 advertised by Device1.

## 59.3.2 Configure IRMP Route Redistribution

### Network Requirements

- Device3 establishes OSPF neighbors with Device2, and advertises direct routes of the interface 200.0.0.0/24 and 210.0.0.0/24 to Device2.
- Device1 establishes IRMP neighbors with Device2. When Device2 redistributes OSPF route to IRMP, use routing policy to advertise the route 200.0.0.0/24 instead of the

route 210.0.0.0/24 to Device1.

## Network Topology



Figure 59 Network Topology for IRMP Route Redistribution

## Configuration Steps

Step 1: Configure IP addresses for the ports. (Omitted)

Step 2: Configure OSPF.

#Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#exit
```

#Configure Device3.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 200.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 210.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#exit
```

#View the routing table of Device 2.

```
Device2#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
U - Per-user Static route
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 1.0.0.0/24 is directly connected, 07:39:21, vlan2
C 2.0.0.0/24 is directly connected, 00:03:36, vlan3
C 127.0.0.8 is directly connected, 57:04:58, lo0
O 200.0.0.0/24 [110/2] via 2.0.0.2, 00:01:10, vlan3
O 210.0.0.0/24 [110/2] via 2.0.0.2, 00:01:10, vlan3
```

According to the routing table, Device2 learns the OSPF route 200.0.0.0/24 and 210.0.0.0/24 advertised by Device3.

Step 3: Configure IRMP.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#router irmp 100
```

```
Device1(config-irmp)#network 1.0.0.0 0.0.0.255
Device1(config-irmp)#exit
```

#Configure Device2.

```
Device2(config)#router irmp 100
Device2(config-irmp)#network 1.0.0.0 0.0.0.255
Device2(config-irmp)#exit
```

#View the information of IRMP neighbors on Device1.

```
Device1#show ip irmp neighbor
IP-IRMP neighbors for process 100 Total neighbor 1
Address      Interface      Hold(s)  Uptime  SeqNum  Srtt(ms)  Rto(s)
1.0.0.2      vlan2          11       00:01:19  1       16        2
```

IRMP neighbor has been successfully established between Device1 and Device2.

Step 4: Configure IRMP to redistribute OSPF routes and associate routing policy.

#Configure routing policy on Device2 to match the ACL that permits the route 200.0.0.0/24 only, and associate this routing policy when IRMP redistributes OSPF routes.

```
Device2(config)#ip access-list standard 1
Device2(config-std-nacl)#permit 200.0.0.0 0.0.0.255
Device2(config-std-nacl)#exit
Device2(config)#route-map ospf_to_irmp
Device2(config-route-map)#match ip address 1
Device2(config-route-map)#exit
Device2(config)#router irmp 100
Device2(config-irmp)#redistribute ospf 100 route-map ospf_to_irmp
Device2(config-irmp)#exit
```

---

## Note

- When configuring a routing policy, both the prefix list and ACL can create matching rules. The difference is that the prefix list can exactly match the routing mask.
- 

Step 5: Check the result.

#View the RMP topology table on Device2.

```
Device2#show ip irmp topology
IP-IRMP Topology Table for process 100
Codes: P - Passive, A - Active, H - Holddown, D - Hidden
> - FIB route, * - FIB successor

P >1.0.0.0/24, 1 successors, FD is 28160
   *via Connected (28160/0), vlan2
P 200.0.0.0/24, 1 successors, FD is 28160
   via RedisOSPF 100 (28160/0)
```

According to the result, Device2 has successfully redistributed OSPF route to IRMP.

#View topology table and routing table on Device1.

```
Device1#show ip irmp topology
```

```
IP-IRMP Topology Table for process 100
Codes: P - Passive, A - Active, H - Holddown, D - Hidden
       > - FIB route, * - FIB successor

P>1.0.0.0/24, 1 successors, FD is 28160
   *via Connected (28160/0), vlan2
P>200.0.0.0/24, 1 successors, FD is 30720
   *via 1.0.0.2 (30720/28160), vlan2

Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 1.0.0.0/24 is directly connected, 07:47:01, vlan2
C 127.0.0.0/8 is directly connected, 07:55:23, lo0
Ex 200.0.0.0/24 [170/30720] via 1.0.0.2, 00:00:06, vlan2
```

According to the result, Device1 learns the route 200.0.0.0/24.

---

## Caution

- In practical applications, if the autonomous system has 2 or more edge routers, directly redistributing routes between different routing protocols is not recommended. When configuration is necessary, routing control policies such as filtering and summarization are required on the edge routers of the autonomous system to avoid routing loops.
- 

### 59.3.3 Configure IRMP Metric Offset

#### Network Requirements

- Run IRMP protocol between Device1, Device2, Device3 and Device4 for interaction.
- Device1 learns the route 200.0.0.0/24 from both Device2 and Device3 at the same time.
- It is required to configure the routing metric offset in the receiving direction on Device1 to make Device1 first select the route advertised by Device2.

#### Network Topology

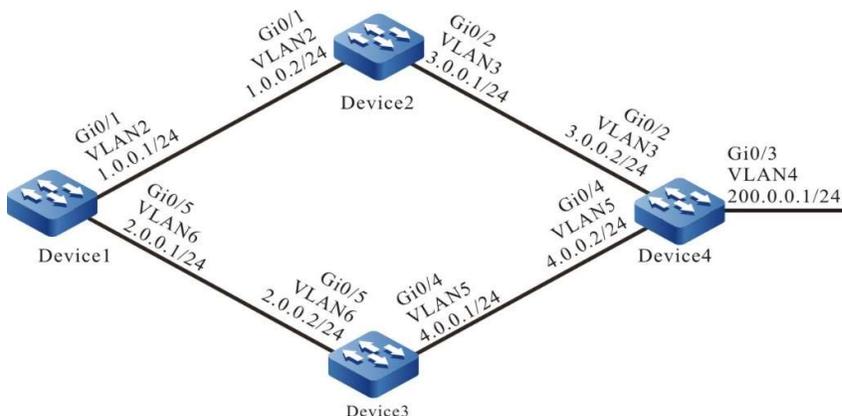


Figure 59 Network Topology for IRMP Metric Offset

### Configuration Steps

Step 1: Configure IP addresses for the ports. (Omitted)

Step 2: Configure IRMP.

#### #Configure Device1.

```
Device1#configure terminal
Device1(config)#router irmp 100
Device1(config-irmp)#network 1.0.0.0 0.0.0.255
Device1(config-irmp)#network 2.0.0.0 0.0.0.255
Device1(config-irmp)#exit
```

#### #Configure Device2.

```
Device2#configure terminal
Device2(config)#router irmp 100
Device2(config-irmp)#network 1.0.0.0 0.0.0.255
Device2(config-irmp)#network 3.0.0.0 0.0.0.255
Device2(config-irmp)#exit
```

#### #Configure Device3.

```
Device3#configure terminal
Device3(config)#router irmp 100
Device3(config-irmp)#network 2.0.0.0 0.0.0.255
Device3(config-irmp)#network 4.0.0.0 0.0.0.255
Device3(config-irmp)#exit
```

#### #Configure Device4.

```
Device4#configure terminal
Device4(config)#router irmp 100
Device4(config-irmp)#network 3.0.0.0 0.0.0.255
Device4(config-irmp)#network 4.0.0.0 0.0.0.255
Device4(config-irmp)#network 200.0.0.0 0.0.0.255
Device4(config-irmp)#exit
```

#### #View the information of IRMP neighbors on Device1.

```
Device1#show ip irmp neighbor
IP-IRMP neighbors for process 100 Total neighbor 2
Address      Interface      Hold(s)  Uptime      SeqNum  Srtt(ms)  Rto(s)
1.0.0.2     vlan2          11       00:10:37  10      0          2
2.0.0.2     vlan6          12       00:10:15  9       0          2
```

#View the information of IRMP neighbors on Device4.

```
Device4#show ip irmp neighbor
IP-IRMP neighbors for process 100 Total neighbor 2
Address      Interface      Hold(s)  Uptime    SeqNum  Srtt(ms)  Rto(s)
3.0.0.1      vlan3          14       00:11:37  13      0          2
4.0.0.1      vlan5          12       00:10:45  12      0          2
```

Device1 has successfully established IRMP neighbors with Device2 and Device3, and Device4 has successfully established IRMP neighbors with Device2 and Device3.

#View topology table and routing table on Device1.

```
Device1#show ip irmp topology
IP-IRMP Topology Table for process 100
Codes: P - Passive, A - Active, H - Holddown, D - Hidden
> - FIB route, * - FIB successor

P >1.0.0.0/24, 1 successors, FD is 28160
    *via Connected (28160/0), vlan2
P >2.0.0.0/24, 1 successors, FD is 28160
    *via Connected (28160/0), vlan6
P >3.0.0.0/24, 1 successors, FD is 30720
    *via 1.0.0.2 (30720/28160), vlan2
P >4.0.0.0/24, 1 successors, FD is 30720
    *via 2.0.0.2 (30720/512), vlan6
P >200.0.0.0/24, 2 successors, FD is 33280
    *via 2.0.0.2 (33280/30720), vlan6
    *via 1.0.0.2 (33280/30720), vlan2

Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
U - Per-user Static route
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 1.0.0.0/24 is directly connected, 13:16:35, vlan2
C 2.0.0.0/24 is directly connected, 13:19:24, vlan6
E 3.0.0.0/24 [90/30720] via 1.0.0.2, 00:03:22, vlan2
E 4.0.0.0/24 [90/30720] via 2.0.0.2, 00:22:01, vlan6
C 127.0.0.0/8 is directly connected, 22:27:25, lo0
E 200.0.0.0/24 [90/33280] via 2.0.0.2, 00:21:22, vlan6
    [90/33280] via 1.0.0.2, 00:03:22, vlan2
```

There are two load balancing routes leading to the network segment 200.0.0.0/24 in the routing table of Device1. The forwarding paths to this network segment are as follows: Device1→Device2→Device4 and Device1→Device3→Device4.

Step 3: Configure IRMP metric offset.

#Configure an offset list on Device1, and add the metric value by 100 on the interface connected to Device3 for the specified route 200.0.0.0/24, so that the total metric value that passes through Device3 is greater than that passes through Device2.

```
Device1(config)#ip access-list standard 1
Device1(config-std-nacl)#permit 200.0.0.0 0.0.0.255
Device1(config-std-nacl)#exit
Device1(config)#router irmp 100
Device1(config-irmp)#offset-list 1 in 100 vlan 6
Device1(config-irmp)#exit
```

Step 4: Check the result.

#View topology table and routing table on Device1.

```
Device1#show ip irmp topology
IP-IRMP Topology Table for process 100
Codes: P - Passive, A - Active, H - Holddown, D - Hidden
> - FIB route, * - FIB successor

P >1.0.0.0/24, 1 successors, FD is 28160
  *via Connected (28160/0), vlan2
P >2.0.0.0/24, 1 successors, FD is 28160
  *via Connected (28160/0), vlan6
P >3.0.0.0/24, 1 successors, FD is 30720
  *via 1.0.0.2 (30720/28160), vlan2
P >4.0.0.0/24, 1 successors, FD is 30720
  *via 2.0.0.2 (30720/512), vlan6
P >200.0.0.0/24, 2 successors, FD is 33280
  *via 1.0.0.2 (33280/30720), vlan2
  via 2.0.0.2 (33380/30820), vlan6

Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
U - Per-user Static route
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 1.0.0.0/24 is directly connected, 13:33:22, vlan2
C 2.0.0.0/24 is directly connected, 13:36:11, vlan6
E 3.0.0.0/24 [90/30720] via 1.0.0.2, 00:06:56, vlan2
E 4.0.0.0/24 [90/30720] via 2.0.0.2, 00:05:43, vlan6
C 127.0.0.0/8 is directly connected, 22:44:12, lo0
E 200.0.0.0/24 [90/33280] via 1.0.0.2, 00:06:56, vlan2
```

After configuring metric offset, Device1 selects the route 200.0.0.0/24 advertised by Device2.

---

### Note

- Configuring IRMP offset list will result in the reestablishment of neighbors.
- 

## 59.3.4 Configure IRMP Route Filtration

### Network Requirements

- Run IRMP between Device1 and Device2 for route interaction.
- The two routes 2.0.0.0/24 and 3.0.0.0/24 advertised by Device2 are learned on Device1. Yet only the routing information of 2.0.0.0/24 needs to be retained on Device1.

### Network Topology

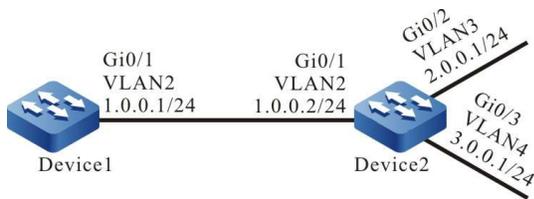


Figure 59 Network Topology for IRMP Route Filtration

### Configuration Steps

Step 1: Configure IP addresses for the ports. (Omitted)

Step 2: Configure IRMP.

#### #Configure Device1.

```
Device1#configure terminal
Device1(config)#router irmp 100
Device1(config-irmp)#network 1.0.0.0 0.0.0.255
Device1(config-irmp)#exit
```

#### #Configure Device2.

```
Device2#configure terminal
Device2(config)#router irmp 100
Device2(config-irmp)#network 1.0.0.0 0.0.0.255
Device2(config-irmp)#network 2.0.0.0 0.0.0.255
Device2(config-irmp)#network 3.0.0.0 0.0.0.255
Device2(config-irmp)#exit
```

#### #View the information of IRMP neighbors on Device1.

```
Device1#show ip irmp neighbor
IP-IRMP neighbors for process 100 Total neighbor 1
Address      Interface      Hold(s)  Uptime    SeqNum  Srtt(ms)  Rto(s)
1.0.0.2      vlan2          11       00:05:00  3       0         2
```

According to the result, IRMP neighbor has been successfully established between Device1 and Device2.

#### #View the routing table of Device1.

```
Device1#show ip irmp topology
IP-IRMP Topology Table for process 100
Codes: P - Passive, A - Active, H - Holddown, D - Hidden
       > - FIB route, * - FIB successor

P >1.0.0.0/24, 1 successors, FD is 28160
   *via Connected (28160/0), vlan2
P >2.0.0.0/24, 1 successors, FD is 30720
   *via 1.0.0.2 (30720/28160), vlan2
P >3.0.0.0/24, 1 successors, FD is 30720
   *via 1.0.0.2 (30720/28160), vlan2

Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 1.0.0.0/24 is directly connected, 00:11:29, vlan2
E 2.0.0.0/24 [90/30720] via 1.0.0.2, 00:07:43, vlan2
E 3.0.0.0/24 [90/30720] via 1.0.0.2, 00:07:40, vlan2
C 127.0.0.0/8 is directly connected, 00:19:50, lo0
```

Device1 learns the routes 2.0.0.0/24 and 3.0.0.0/24.

Step 3: Configure route filtration.

#Configure ACL rules on Device1 to allow the route 2.0.0.0/24 only, and configure association of filter list with this ACL in the incoming direction in IRMP.

```
Device1(config)#ip access-list standard 1
Device1(config-std-nacl)#permit 2.0.0.0 0.0.0.255
Device1(config-std-nacl)#exit
Device1(config)#router irmp 100
Device1(config-irmp)#distribute-list 1 in
Device1(config-irmp)#exit
```

---

### Note

- When configuring route filtration, both the prefix list and ACL can create filtering rules. The difference is that the prefix list can exactly match the routing mask.
- 

Step 4: Check the result.

#View topology table and routing table on Device1.

```
Device1#show ip irmp topology
IP-IRMP Topology Table for process 100
Codes: P - Passive, A - Active, H - Holddown, D - Hidden
> - FIB route, * - FIB successor

P >1.0.0.0/24, 1 successors, FD is 28160
   *via Connected (28160/0), vlan2
P >2.0.0.0/24, 1 successors, FD is 30720
   *via 1.0.0.2 (30720/28160), vlan2

Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 1.0.0.0/24 is directly connected, 00:22:33, vlan2
E 2.0.0.0/24 [90/30720] via 1.0.0.2, 00:04:18, vlan2
C 127.0.0.0/8 is directly connected, 00:30:55, lo0
```

Device1 learns the route 2.0.0.0/24 only. The route 3.0.0.0/24 has been successfully filtered.

---

### Note

- Configuring the command **distribute-list** will result in the reestablishment of IRMP neighbors.
-

## 59.3.5 Configure IRMP Route Summarization

### Network Requirements

- Run IRMP between Device1, Device2, Device3 and Device4 for route interaction.
- Device1 learns two routes, i.e. 100.1.0.0/24 and 100.2.0.0/24, from Device2. In order to reduce the size of the routing table of Device1, Device2 needs to distribute the summarized route 100.0.0.0/14 only to Device1.

### Network Topology

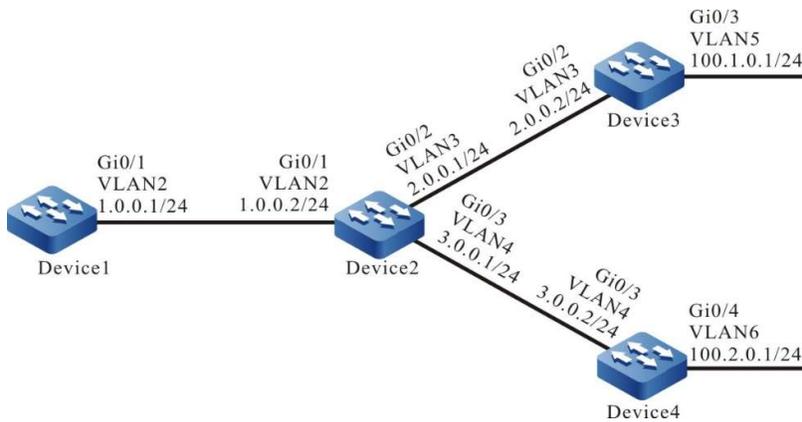


Figure 59 Network Topology for IRMP Route Summarization

### Configuration Steps

Step 1: Configure IP addresses for the ports. (Omitted)

Step 2: Configure IRMP.

#### #Configure Device1.

```
Device1#configure terminal
Device1(config)#router irmp 100
Device1(config-irmp)#network 1.0.0.0 0.0.0.255
Device1(config-irmp)#exit
```

#### #Configure Device2.

```
Device2#configure terminal
Device2(config)#router irmp 100
Device2(config-irmp)#network 1.0.0.0 0.0.0.255
Device2(config-irmp)#network 2.0.0.0 0.0.0.255
Device2(config-irmp)#network 3.0.0.0 0.0.0.255
Device2(config-irmp)#exit
```

#### #Configure Device3.

```
Device3#configure terminal
Device3(config)#router irmp 100
Device3(config-irmp)#network 2.0.0.0 0.0.0.255
Device3(config-irmp)#network 100.1.0.0 0.0.0.255
Device3(config-irmp)#exit
```

#### #Configure Device4.

```
Device4#configure terminal
Device4(config)#router irmp 100
Device4(config-irmp)#network 3.0.0.0 0.0.0.255
Device4(config-irmp)#network 100.2.0.0 0.0.0.255
Device4(config-irmp)#exit
```

#### #View the information of IRMP neighbors on Device2.

```
Device2#show ip irmp neighbor
IP-IRMP neighbors for process 100 Total neighbor 3
Address      Interface      Hold(s)  Uptime    SeqNum  Srtt(ms)  Rto(s)
1.0.0.1      vlan2          11       00:05:04  4       0         2
2.0.0.2      vlan3          14       00:04:42  3       16        2
3.0.0.2      vlan4          11       00:04:00  2       0         2
```

Device2 establishes IRMP neighbors with Device1, Device3 and Device4 respectively.

#### #View the topology table and routing table of Device2.

```
Device2#show ip irmp topology
IP-IRMP Topology Table for process 100
Codes: P - Passive, A - Active, H - Holddown, D - Hidden
> - FIB route, * - FIB successor

P >1.0.0.0/24, 1 successors, FD is 28160
    *via Connected (28160/0), vlan2
P >2.0.0.0/24, 1 successors, FD is 28160
    *via Connected (28160/0), vlan3
P >3.0.0.0/24, 1 successors, FD is 28160
    *via Connected (28160/0), vlan4
P >100.1.0.0/24, 1 successors, FD is 30720
    *via 2.0.0.2 (30720/28160), vlan3
P >100.2.0.0/24, 1 successors, FD is 30720
    *via 3.0.0.2 (30720/28160), vlan4

Device2#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
U - Per-user Static route
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 1.0.0.0/24 is directly connected, 08:12:36, vlan2
C 2.0.0.0/24 is directly connected, 00:36:51, vlan3
C 3.0.0.0/24 is directly connected, 00:12:06, vlan4
E 100.1.0.0/24 [90/30720] via 2.0.0.2, 00:10:03, vlan3
E 100.2.0.0/24 [90/30720] via 3.0.0.2, 00:00:08, vlan4
C 127.0.0.0/8 is directly connected, 57:38:13, lo0
```

#### #View topology table and routing table on Device1.

```
Device1#show ip irmp topology
IP-IRMP Topology Table for process 100
Codes: P - Passive, A - Active, H - Holddown, D - Hidden
> - FIB route, * - FIB successor

P >1.0.0.0/24, 1 successors, FD is 28160
    *via Connected (28160/0), vlan2
P >2.0.0.0/24, 1 successors, FD is 30720
    *via 1.0.0.2 (30720/28160), vlan2
P >3.0.0.0/24, 1 successors, FD is 30720
    *via 1.0.0.2 (30720/28160), vlan2
P >100.1.0.0/24, 1 successors, FD is 33280
    *via 1.0.0.2 (33280/30720), vlan2
P >100.2.0.0/24, 1 successors, FD is 33280
    *via 1.0.0.2 (33280/30720), vlan2

Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
```

U - Per-user Static route  
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

```
C 1.0.0.0/24 is directly connected, 08:09:15, vlan2
E 2.0.0.0/24 [90/30720] via 1.0.0.2, 00:13:19, vlan2
E 3.0.0.0/24 [90/30720] via 1.0.0.2, 00:13:17, vlan2
E 100.1.0.0/24 [90/33280] via 1.0.0.2, 00:12:53, vlan2
E 100.2.0.0/24 [90/33280] via 1.0.0.2, 00:02:57, vlan2
C 127.0.0.0/8 is directly connected, 08:17:36, lo0
```

Both Device1 and Device2 have learned the routes 100.1.0.0/24 and 100.2.0.0/24.

Step 3: Configure IRMP route summarization.

#On Device2, configure IRMP summarized route 100.0.0.0/14 on the interface connected to Device1.

```
Device2(config)#interface vlan 2
Device2(config-if-vlan2)#ip summary-address irmp 100 100.0.0.0 255.252.0.0
Device2(config-if-vlan2)#exit
```

Step 4: Check the result.

#View the RMP topology table on Device2.

```
Device2#show ip irmp topology
IP-IRMP Topology Table for process 100
Codes: P - Passive, A - Active, H - Holddown, D - Hidden
> - FIB route, * - FIB successor

P >1.0.0.0/24, 1 successors, FD is 28160
    *via Connected (28160/0), vlan2
P >2.0.0.0/24, 1 successors, FD is 28160
    *via Connected (28160/0), vlan3
P >3.0.0.0/24, 1 successors, FD is 28160
    *via Connected (28160/0), vlan4
P 100.0.0.0/14, 1 successors, FD is 30720
    via AddrSumm (30720/0)
P >100.1.0.0/24, 1 successors, FD is 30720
    *via 2.0.0.2 (30720/28160), vlan3
P >100.2.0.0/24, 1 successors, FD is 30720
    *via 3.0.0.2 (30720/28160), vlan4
```

A summarized route 100.0.0.0/14 is generated on Device2.

#View topology table and routing table on Device1.

```
Device1#show ip irmp topology
IP-IRMP Topology Table for process 100
Codes: P - Passive, A - Active, H - Holddown, D - Hidden
> - FIB route, * - FIB successor

P >1.0.0.0/24, 1 successors, FD is 28160
    *via Connected (28160/0), vlan2
P >2.0.0.0/24, 1 successors, FD is 30720
    *via 1.0.0.2 (30720/28160), vlan2
P >3.0.0.0/24, 1 successors, FD is 30720
    *via 1.0.0.2 (30720/28160), vlan2
P >100.0.0.0/14, 1 successors, FD is 33280
    *via 1.0.0.2 (33280/30720), vlan2

Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
U - Per-user Static route
```

O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

```
C 1.0.0.0/24 is directly connected, 08:18:49, vlan2
E 2.0.0.0/24 [90/30720] via 1.0.0.2, 00:04:54, vlan2
E 3.0.0.0/24 [90/30720] via 1.0.0.2, 00:04:54, vlan2
E 100.0.0.0/14 [90/33280] via 1.0.0.2, 00:04:54, vlan2
C 127.0.0.0/8 is directly connected, 08:27:10, lo0
```

According to the result, only the summarized route 100.0.0.0/14 is found in the routing table of Device1. There are no corresponding detail routes 100.1.0.0/24 and 100.2.0.0/24.

---

## Note

- Configuring IRMP route summarization in interface mode will result in the reestablishment of neighbors.
- 

### 59.3.6 Configure IRMP Load Balancing

#### Network Requirements

- Run IRMP between Device1, Device2, Device3 and Device4 for route interaction.
- Device1 learns the route 200.0.0.0/24 from Device2 and Device3 at the same time. Modify the bandwidth of Device1's interface vlan4 so that Device1 selects the route 200.0.0.0/24 learned from Device2.
- Device1 is required to forward data to the network segment 200.0.0.0/24 on the two lines Device1→Device2→Device4 and Device1→Device3→Device4.

#### Network Topology

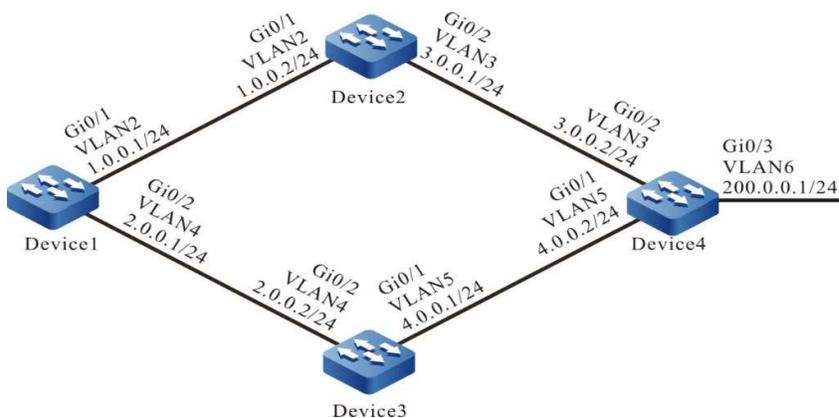


Figure 59 Network Topology for IRMP Unequal-cost Load Balancing

#### Configuration Steps

Step 1: Configure IP addresses for the ports. (Omitted)

Step 2: Configure IRMP.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#router irmp 100
Device1(config-irmp)#network 1.0.0.0 0.0.0.255
Device1(config-irmp)#network 2.0.0.0 0.0.0.255
Device1(config-irmp)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#router irmp 100
Device2(config-irmp)#network 1.0.0.0 0.0.0.255
Device2(config-irmp)#network 3.0.0.0 0.0.0.255
Device2(config-irmp)#exit
```

#Configure Device3.

```
Device3#configure terminal
Device3(config)#router irmp 100
Device3(config-irmp)#network 2.0.0.0 0.0.0.255
Device3(config-irmp)#network 4.0.0.0 0.0.0.255
Device3(config-irmp)#exit
```

#Configure Device4.

```
Device4#configure terminal
Device4(config)#router irmp 100
Device4(config-irmp)#network 3.0.0.0 0.0.0.255
Device4(config-irmp)#network 4.0.0.0 0.0.0.255
Device4(config-irmp)#network 200.0.0.0 0.0.0.255
Device4(config-irmp)#exit
```

#View the information of IRMP neighbors on Device1.

```
Device1#show ip irmp neighbor
IP-IRMP neighbors for process 100 Total neighbor 2
Address      Interface      Hold(s)  Uptime    SeqNum  Srtt(ms)  Rto(s)
1.0.0.2      vlan2          11       00:10:37  10      0          2
2.0.0.2      vlan4          12       00:10:15  9        0          2
```

#View the information of IRMP neighbors on Device4.

```
Device4#show ip irmp neighbor
IP-IRMP neighbors for process 100 Total neighbor 2
Address      Interface      Hold(s)  Uptime    SeqNum  Srtt(ms)  Rto(s)
3.0.0.1      vlan3          14       00:11:37  13      0          2
4.0.0.1      vlan5          12       00:10:45  12      0          2
```

Device1 has successfully established IRMP neighbors with Device2 and Device3, and Device4 has successfully established IRMP neighbors with Device2 and Device3.

#View topology table and routing table on Device1.

```
Device1#show ip irmp topology
IP-IRMP Topology Table for process 100
Codes: P - Passive, A - Active, H - Holddown, D - Hidden
> - FIB route, * - FIB successor

P >1.0.0.0/24, 1 successors, FD is 28160
   *via Connected (28160/0), vlan2
```

```

P>2.0.0.0/24, 1 successors, FD is 28160
  *via Connected (28160/0), vlan4
P>3.0.0.0/24, 1 successors, FD is 30720
  *via 1.0.0.2 (30720/28160), vlan2
P>4.0.0.0/24, 1 successors, FD is 30720
  *via 2.0.0.2 (30720/512), vlan4
P>200.0.0.0/24, 2 successors, FD is 33280
  *via 2.0.0.2 (33280/30720), vlan4
  *via 1.0.0.2 (33280/30720), vlan2

Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 1.0.0.0/24 is directly connected, 13:16:35, vlan2
C 2.0.0.0/24 is directly connected, 13:19:24, vlan4
E 3.0.0.0/24 [90/30720] via 1.0.0.2, 00:03:22, vlan2
E 4.0.0.0/24 [90/30720] via 2.0.0.2, 00:22:01, vlan4
C 127.0.0.0/8 is directly connected, 22:27:25, lo0
E 200.0.0.0/24 [90/33280] via 2.0.0.2, 00:21:22, vlan4
  [90/33280] via 1.0.0.2, 00:03:22, vlan2

```

There are two routes leading to the network segment 200.0.0.0/24 in the routing table of Device1. The forwarding paths to this network segment are as follows: Device1→Device2→Device4 and Device1→Device3→Device4.

Step 3: Modify interface bandwidth.

#Modify the bandwidth of the interface connected to Device1 and Device3 as 10000Kbps.

```

Device1(config)#interface vlan 4
Device1(config-if-vlan4)#bandwidth 10000
Device1(config-if-vlan4)#exit

```

#View topology table and routing table on Device1.

```

Device1#show ip irmp topology
IP-IRMP Topology Table for process 100
Codes: P - Passive, A - Active, H - Holddown, D - Hidden
       > - FIB route, * - FIB successor

P>1.0.0.0/24, 1 successors, FD is 28160
  *via Connected (28160/0), vlan2
P>2.0.0.0/24, 1 successors, FD is 258560
  *via Connected (258560/0), vlan4
P>3.0.0.0/24, 1 successors, FD is 30720
  *via 1.0.0.2 (30720/28160), vlan2
P>4.0.0.0/24, 1 successors, FD is 261120
  *via 2.0.0.2 (261120/28160), vlan4
P>200.0.0.0/24, 2 successors, FD is 33280
  *via 1.0.0.2 (33280/30720), vlan2
  via 2.0.0.2 (263680/30720), vlan4

Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 1.0.0.0/24 is directly connected, 28:44:11, vlan2
C 2.0.0.0/24 is directly connected, 00:14:05, vlan4
E 3.0.0.0/24 [90/30720] via 1.0.0.2, 00:10:11, vlan2
E 4.0.0.0/24 [90/284160] via 2.0.0.2, 00:07:57, vlan4
C 127.0.0.0/8 is directly connected, 22:26:51, lo0
E 200.0.0.0/24 [90/33280] via 1.0.0.2, 00:10:11, vlan2

```

After configuring metric offset, Device1 selects the route 200.0.0.0/24 advertised by Device2.

Step 4: Configure IRMP unequal-cost load balancing.

#On Device1, configure the transformation factor of load balancing as 100.

```
Device1(config)#router irmp 100
Device1(config-irmp)#variance 100
Device1(config-irmp)#exit
```

For detailed introduction to the transformation factor of load balancing, see the load balancing section of the IRMP function configuration part.

Step 5: Check the result.

#View topology table and routing table on Device1.

```
Device1#show ip irmp topology
IP-IRMP Topology Table for process 100
Codes: P - Passive, A - Active, H - Holddown, D - Hidden
> - FIB route, * - FIB successor

P >1.0.0.0/24, 1 successors, FD is 28160
    *via Connected (28160/0), vlan2
P >2.0.0.0/24, 1 successors, FD is 28160
    *via Connected (28160/0), vlan4
P >3.0.0.0/24, 1 successors, FD is 30720
    *via 1.0.0.2 (30720/28160), vlan2
P >4.0.0.0/24, 1 successors, FD is 284160
    *via 2.0.0.2 (284160/28160), vlan4
P >200.0.0.0/24, 2 successors, FD is 33280
    *via 1.0.0.2 (33280/30720), vlan2
    *via 2.0.0.2 (263680/30720), vlan4

Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
U - Per-user Static route
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 1.0.0.0/24 is directly connected, 28:47:15, vlan2
C 2.0.0.0/24 is directly connected, 00:17:08, vlan4
E 3.0.0.0/24 [90/30720] via 1.0.0.2, 00:13:15, vlan2
E 4.0.0.0/24 [90/284160] via 2.0.0.2, 00:11:00, vlan4
C 127.0.0.0/8 is directly connected, 220:29:54, lo0
E 200.0.0.0/24 [90/33280] via 1.0.0.2, 00:13:15, vlan2
    [90/263680] via 2.0.0.2, 00:00:12, vlan4
```

The route 200.0.0.0/24 on Device1 shows unequal-cost load balancing. The data will have load transmission on these two paths by the inverse ratio of metric value.

# 60 BGP

---

## 60.1 Overview

BGP (Border Gateway Protocol) is a routing protocol which can be used to exchange Network Layer Reachability Information (NLRI) between Autonomous Systems (AS). IGPs (Internal Gateway Protocols), e.g. RIP, OSPF and IS-IS, aim to look for exact paths, with network node (such as router, three-layer switch, and multi-NIC host) being the path finding unit. EGPs (External Gateway Protocols) focus on controlling routing direction, with AS network being the unit.

BGPs can be used for interconnection between AS networks to provide routing information exchange between AS. They are widely applied in large network aggregation and network core. This application level makes BGP have the following characteristics compared to IGP:

- BGP uses TCP protocol to transmit packets, and the service port number is 179. TCP guarantees the reliability of transmission. Therefore, a separate transmission control policy is not required to ensure the reliability of information;
- BGP updates routes through increment. That is to say, only when routing attributes change or routes are added or deleted, such routing change will be advertised to neighbors. This greatly reduces the network bandwidth occupied by BGP to propagate routes;
- BGP is an AS-based distance vector protocol. It deals with routing loops by carrying AS path attributes in routing packets;
- BGP route has various attributes. You can control route filtering and selection by applying routing policies to modify these attributes;
- BGP has two types of neighbor, i.e. IBGP and EBGP. They have different route advertising and selection policies.

## 60.2 BGP function configuration

Table 60 BGP Function Configuration List

Configuration Task	
Configure BGP Neighbor	Configure IBGP Neighbor
	Configure EBGP Neighbor

Configuration Task	
	Configure Passive BGP Neighbor
	Configure MP-BGP Neighbor
	Configure MD5 Authentication of BGP Neighbor
Configure BGP Route Generation	Configure BGP to Distribute Local Route
	Configure BGP Route Redistribution
	Configure BGP to Distribute Default Route
Configure BGP Route Control	Configure BGP to Distribute Aggregated Route
	Configure Administrative Distance of BGP Route
	Configure Routing Policy of BGP Neighbors in Outgoing Direction
	Configure Routing Policy of BGP Neighbors in Incoming Direction
	Configure the Maximum Number of Routing Entries Received by BGP Neighbors
	Configure the Maximum Number of BGP Load Balancing Entries
Configure BGP Route Attributes	Configure BGP Route Weight
	Configure MED Attributes of BGP Route
	Configure Local-Preference Attributes of BGP Route
	Configure AS_PATH Attributes of BGP Route
	Configure NEXT-HOP Attributes of BGP Route
	Configure Community Attributes of BGP Route
Configure BGP Network Optimization	Configure Keepalive Time of BGP Neighbor
	Configure BGP Route Detection Time

Configuration Task	
	Configure Fast Disconnection of EBGP Neighbor
	Configure BGP Route Dampening Function
	Configure BGP Neighbor Refresh Capability
	Configure Soft Resetting Capability of BGP Neighbor
	Configure ORF Capability of BGP Neighbor
Configure Large BGP Network	Configure BGP Peer Group
	Configure BGP Route Reflector
	Configure BGP Confederation
Configure BGP GR	Configure BGP GR Helper
Configure BGP to Coordinate with BFD	Configure EBGP to Coordinate with BFD
	Configure IBGP to Coordinate with BFD

## 60.2.1 Configure BGP Neighbor

### Configuration Condition

Before configuring BGP neighbors, do the following:

- The link layer protocol has been configured to ensure normal communication at the link layer.
- Configure address of interface at network layer so that neighbor network nodes are reachable at the network layer.

### Configure IBGP Neighbor

#### 1. Basic configuration

To configure IBGP neighbor, you are required to specify the same AS of neighbor as that of this device. Router ID can be configured for the device. It is used to uniquely mark a BGP device when establishing BGP session. When Router ID is not configured, the device will select one based interface address according to by following principles:

- Firstly, select the largest IP address from the Loopback interface as Router ID;

- If no Loopback interface is configured for IP address, select the largest IP addresses from other interfaces as Router ID;
- Only when the interface is UP can the interface address be selected as Router ID.

Table 60 Configuring IBGP Neighbor

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable the BGP protocol and enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	Mandatory By default, BGP is disabled.
Configure BGP device ID	<b>bgp router-id</b> <i>router-id</i>	Optional By default, the device makes selections according to interface address. In particular, Loopback interface and large IP address have a higher priority.
Configure IBGP Neighbor	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>remote-as</b> <i>as-number</i>	Mandatory By default, no IBGP neighbor is created.
Activate IBGP neighbor's capability of receiving and sending IPv4 unicast route	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>activate</b>	Optional By default, IBGP neighbor's capability of receiving and sending IPv4 unicast route is automatically activated.
Description of configuring IBGP neighbor	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>description</b> <i>description-string</i>	Optional By default, there is no description of IBGP neighbor.

## 2. Configure source address of TCP session

BGP uses TCP as transmission protocol. Featured by reliable transmission, TCP can effectively ensure that BGP protocol packets are correctly transmitted to the neighbors.

Table 60 Configuring Source Address of TCP Session

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable the BGP protocol and enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Configure IBGP Neighbor	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>remote-as</b> <i>as-number</i>	Mandatory By default, no IBGP neighbor is created.
Configure source address for TCP session of IBGP neighbors	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>update-source</b> { <i>interface-name</i>   <i>ip-address</i> }	Mandatory By default, the TCP session automatically selects the address of the route's output interface as source address.

### Note

- When there is load balancing route, source address of TCP session is required to be configured between BGP neighbors. When the TCP source address is not configured, different output interfaces may be used as their source addresses because neighbors have different optimal routes. As a result, BGP session cannot be successfully established within a period of time.

## Configure EBGP Neighbor

### 1. Basic configuration

To configure EBGP neighbor, you are required to specify different AS of neighbor from that of this device.

Table 60 Configuring EBGP Neighbor

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Enable the BGP protocol and enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Configure EBGP Neighbor	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>remote-as</b> <i>as-number</i>	Mandatory By default, no EBGP neighbor is created.

## 2. Configure Indirect EBGP Neighbor

Located in different operation networks, EBGP neighbors are often connected via a direct physical link. Thus, the default TTL value of IP packets communicated between EBGP neighbors is 1. If they are in the indirect operation network, you can set the TTL value of IP packets via a configuration command to allow BGP connection.

Table 60 Configuring Indirect EBGP Neighbor

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Configure EBGP Neighbor	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>remote-as</b> <i>as-number</i>	Mandatory By default, no EBGP neighbor is created.
Configure source address for TCP session of EBGP neighbors	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>update-source</b> { <i>interface-name</i>   <i>ip-address</i> }	Optional By default, the TCP session automatically selects the address of the route's output interface as source address.
allow connection between indirect EBGP neighbors	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>ebgp-multihop</b> [ <i>ttl-value</i> ]	Mandatory By default, EBGP neighbor relation between indirect devices is not allowed.

## Configure Passive BGP Neighbor

The passive neighbor function is required in the special application environment. After passive neighbor is applied, BGP will not actively initiate a TCP connection request to establish BGP neighbor. The neighbor relation cannot be built until the neighbor actively issues a connection request. By default, the two neighbors will actively initiate connections to each other. When there is a conflict between the connections, a TCP connection will be selected to create a BGP session. Before configuring passive BGP neighbors, you need to configure BGP neighbors.

● Table 60 Configuring Passive BGP Neighbor

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Configure BGP Neighbor	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>remote-as</b> <i>as-number</i>	Mandatory By default, no BGP neighbor is created.
Configure Passive BGP Neighbor	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>passive</b>	Mandatory By default, no passive neighbor is enabled.

## Configure MP-BGP Neighbor

By default, BGP neighbors are activated under the IPv4 unicast address family. They have the ability of sending and receiving IPv4 unicast routes. For other address families, such as multicast address family, VRF address family, and LS unicast address cluster, neighbors need to be activated through a configuration command so that they can send and receive corresponding routes. Before configuring MP-BGP neighbors, you need to configure BGP neighbors.

Table 60 Configuring MP-BGP Neighbor

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Configure BGP Neighbor	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>remote-as</b> <i>as-number</i>	Mandatory By default, no BGP neighbor is created.
Enter the BGP IPv4 multicast configuration mode	<b>address-family ipv4 multicast</b>	Mandatory By default, unicast address family mode shows after entering the BGP configuration mode.
Activate neighbors under BGP IPv4 multicast address family	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>activate</b>	Mandatory By default, global neighbors are not activated under multicast address family.
Exit the BGP IPv4 multicast configuration mode	<b>exit-address-family</b>	-
Enter the BGP IPv4 VRF configuration mode	<b>address-family ipv4 vrf</b> <i>vrf-name</i>	-
Configure neighbors under BGP IPv4 VRF address family	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>remote-as</b> <i>as-number</i>	Mandatory By default, no BGP neighbor is created.
Activate neighbors under IPv4 VRF address family	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>activate</b>	Optional By default, the neighbors under BGP IPv4 VRF configuration mode have been activated.
Exit the BGP IPv4 VRF configuration mode	<b>exit-address-family</b>	-
Enter the BGP LS configuration mode	<b>address-family link-state unicast</b>	-

Step	Command	Description
Activate neighbors under BGP LS unicast address family	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>activate</b>	Mandatory By default, global neighbors are not activated under VPN address family.
Exit the BGP LS configuration mode	<b>exit-address-family</b>	-

### Note

- Neighbors configured in BGP configuration mode and BGP IPv4 unicast configuration mode are global neighbors, and those configured in BGP IPv4 VRF configuration mode belong to the VRF address family only.

### Configure MD5 Authentication of BGP Neighbor

BGP supports the configuration of MD5 authentication so as to protect the information exchange between neighbors. MD5 authentication is completed by TCP transmission protocol. To establish TCP connection, both neighbors must be configured with the same MD5 authentication password. Otherwise, TCP connection cannot be established after the TCP transmission protocol fails in MD5 authentication. Before configuring MD5 authentication for BGP neighbors, you need to configure BGP neighbors.

Table 60 Configuring MD5 Authentication for BGP Neighbor

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Configure BGP Neighbor	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>remote-as</b> <i>as-number</i>	Mandatory By default, no BGP neighbor is created.
Configure MD5 Authentication of BGP Neighbor	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>password</b> [ 0   7 ] <i>password-string</i>	Mandatory

Step	Command	Description
		By default, there is no MD5 authentication between BGP neighbors.

## 60.2.2 Configure BGP Route Generation

### Configuration Condition

Before configuring BGP route generation, ensure that:

- Enable BGP protocol;
- Configure BGP neighbor and successfully establish and connect a session.

### Configure BGP to Distribute Local Route

BGP can import route from IP routing table into BGP routing table through the **network** command. Only when there is an entry in the IP routing table that fully matches the **network** prefix and mask, will the route be imported into the BGP routing table and distributed.

When distributing locate routes, you can apply a routing map for the routes or specify such routes as backdoor routes. Backdoor route deems EBGP route as local BGP route and uses the administrative distance of local route. In this case, IGP route is allowed to precede EBGP route, and the backdoor route will not advertise it to EBGP neighbors.

Table 60 Configuring BGP to Distribute Local Route

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Configure BGP to Distribute Local Route	<b>network</b> <i>ip-address mask</i> [ <b>route-map</b> <i>rtmap-name</i> [ <b>backdoor</b> ]   <b>backdoor</b> ]	Mandatory By default, BGP doesn't distribute any local route.

### Note

- The Origin attribute of of the local route distributed by BGP is IGP.

- After using the **network backdoor** command on EBGp routes, the EBGp route administrative distance will become the local route administrative distance (by default, the EBGp route administrative distance is 20, and the local route administrative distance is 200), which is lower than the default IGP route administrative distance. In this case, the IGP route will be preferred, and a backdoor link will be created between EBGp neighbors.
- When BGP distributes local routes and applies the routing map, the match options supported include as-path, community, extcommunity, ip address, ip nexthop, and metric, and the set options supported include as-path, comm-list, community, extcommunity, ip next-hop, local-preference, metric, origin, and weight.

### Configure BGP Route Redistribution

BGP is not responsible for learning routes. Instead, it focuses on controlling routing direction by managing route attributes. Therefore, BGP generates BGP routes for advertisement to neighbors by redistributing IGP. BGP can apply the routing map while redistributing IGP routes.

Table 1 Configuring BGP Route Redistribution

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Configure BGP to redistribute IGP routes	<b>redistribute</b> { <b>connected</b>   <b>irmp</b> <i>as-number</i>   <b>isis</b> [ <i>area-tag</i> ] [ <b>match</b> <i>isis-level</i> ]   <b>ospf</b> <i>as-number</i> [ <b>match</b> <i>route-subtype</i> ]   <b>rip</b>   <b>static</b> } [ <b>route-map</b> <i>map-name</i> / <b>metric</b> <i>value</i> ]	Mandatory By default, BGP doesn't redistribute any other IGP routes.

### Note

- The Origin attribute of the IGP route distributed by BGP is INCOMPLETE.
- When BGP redistributes other protocols and applies the routing map, the match options supported include as-path, community, extcommunity, ip address, ip nexthop, and metric, and the set options supported include as-path, comm-list, community, extcommunity, ip next-hop, local-preference, metric, origin, and weight.

### Configure BGP to Distribute Default Route

Before distributing a default route to neighbors, BGP is required to import a default route. This can be done by the following two manners: generate the default route of BGP via the command **neighbor default-originate**; redistribute the default route of other protocols via the command **default-information originate**.

The default route generated by the **neighbor default-originate** command is a route of 0.0.0.0/0 automatically generated through BGP. The default route redistributed by the **default-information originate** command is a route of 0.0.0.0/0 generated when BGP imports the redistributed protocol.

Table 60 Configuring BGP to Distribute Default Route

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Configure BGP to generate default route	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>default-originate</b> [ <b>route-map</b> <i>rmap-name</i> ]	Mandatory By default, BGP doesn't generate default route.
Configure BGP to redistribute the default route of other protocols	<b>default-information originate</b>	Mandatory By default, BGP doesn't redistribute the default route of other protocols.

### Note

- When configuring BGP to redistribute the default route of other protocols, it is required to configure route redistribution.
- You can apply the routing map for the route when configuring BGP to generate a default route.
- When BGP generates default route and applies the routing map, the set options supported include as-path, comm-list, community, extcommunity, ip next-hop, local-preference, metric, origin, and weigh.

## 60.2.3 Configure BGP Route Control

### Configuration Condition

Before configuring BGP route control, ensure that:

- Enable BGP protocol;
- Configure BGP neighbor and successfully establish and connect a session.

### Configure BGP to Distribute Aggregated Route

In large BGP networks, in order to reduce the number of routes advertised to neighbors or effectively control the routing process of BGP, it is required to configure BGP aggregated route.

Table 60 Configuring BGP to Distribute Aggregated Route

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Configure BGP to Distribute Aggregated Route	<b>aggregate-address</b> <i>ip-address mask</i> [ <b>as-set</b> / <b>summary-only</b> / <b>route-map</b> <i>rtmap-name</i> ]	Mandatory By default, route aggregation is disabled for BGP.

---

#### Note

- When BGP distributes aggregated routes, the scale of route advertisement can be reduced by specifying the **summary-only** command option to advertise aggregated routes only.
  - The aggregated route with AS\_PATH attribute can be generated by specifying the **as-set** command option.
  - More attributes can be set for the aggregated routes by applying routing map to them.
- 

### Configure Administrative Distance of BGP Route

Each protocol in the IP routing table has an administrative distance for routing control. The smaller the value, the higher the priority. BGP affects routing by configuring administrative distance for routes in the specified network segment. The administrative distances covered by the routes in the specified network segment will all be modified. At the same time, you may use ACL to effectively filter the network segment so that only the administrative distances in the network segment allowed by ACL can be modified.

The command **distance bgp** can be used to modify the administrative distance of BGP's external, internal and local routes, while the command **distance** is used to change that of the routes in the specified network

segment. The command **distance** precedes **distance bgp**. The network segment configured to be covered by **distance** uses the administrative distance specified by this command, and that uncovered adopts the administrative distance set via **distance bgp**.

Table 2 Configuring BGP Route Administrative Distance

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Configure BGP to modify the default administrative distance	<b>distance bgp</b> <i>external-distance internal-distance local-distance</i>	Optional
Configure administrative distance of the specified network segment	<b>distance</b> <i>administrative-distance ip-address mask [ acl-name ]</i>	By default, the administrative distance of EBGp route is 20, that of IBGP 200, and that of local route 200.

### Configure Routing Policy of BGP Neighbors in Outgoing Direction

BGP route advertisement or routing relies on its powerful route attributes. When advertising routes to neighbors, you can modify route attributes or filter some routes by applying corresponding policies.

Currently, the policies that can be applied in the outgoing direction include:

- distribute-list: distribution list;
- filter-list: filter list with AS\_PATH attribute;
- Prefix-list: IP prefix list;
- route-map: routing map.

Table 3 Configuring Routing Policy of BGP Neighbors in Outgoing Direction

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-

Step	Command	Description
Apply distribution list in the outgoing direction	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>distribute-list</b> <i>access-list-name</i> <b>out</b>	Multiple choice (distribution list and IP prefix list cannot be configured at the same time)
Apply the filter list with AS_PATH attribute in the outgoing direction	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>filter-list</b> <i>aspath-list-name</i> <b>out</b>	
Apply IP prefix list in the outgoing direction	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>prefix-list</b> <i>prefix-list-name</i> <b>out</b>	By default, the routing policy of BGP neighbors in the outgoing direction is not configured.
Apply routing map in the outgoing direction	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>route-map</b> <i>rtmap-name</i> <b>out</b>	

## Note

- After configuring the routing policy of BGP neighbors in the outgoing direction, it is required to reset the neighbors to make it take effect.
- When applying routing map in the outgoing direction of route reflector, only NEXT-HOP attribute can be changed.
- For the configuration of filter list, see the policy tools-configure AS-PATH list section.
- When configuring policy for neighbors in the outgoing direction, you can configure multiple policies at the same time. For BGP, the following sequence applies: **distribute-list**, **filter-list**, **prefix-list**, and **route-map**. After the first policy is rejected, the following policy will not be implemented. Only after all the policies configured pass will the routing information be advertised.
- For the routing map applied in the outgoing direction of BGP, the match options supported include as-path, community, extcommunity, ip address, ip nexthop, and metric, and the set options supported include as-path, comm-list, community, extcommunity, ip next-hop, local-preference, metric, origin, and weight.

## Configure Routing Policy of BGP Neighbors in Incoming Direction

BGP can use policies to filter the routing information received or modify its attributes. Like the outgoing direction, four policies are supported in the incoming direction:

- distribute-list: distribution list;
- filter-list: filter list with AS\_PATH attribute;
- Prefix-list: IP prefix list;

- route-map: routing map.

Table 4 Configuring Application Policy of BGP Neighbors in Incoming Direction

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Apply distribution list in the incoming direction	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>distribute-list</b> <i>access-list-name</i> <b>in</b>	Multiple choice (distribution list and IP prefix list cannot be configured at the same time)  By default, no policy is specified in the incoming direction.
Apply the filter list with AS_PATH attribute in the incoming direction	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>filter-list</b> <i>aspath-list-name</i> <b>in</b>	
Apply IP prefix list in the incoming direction	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>prefix-list</b> <i>prefix-list-name</i> <b>in</b>	
Apply routing map in the incoming direction	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>route-map</b> <i>rtmap-name</i> <b>in</b>	

## Note

- After configuring the routing policy of BGP neighbors in the incoming direction, it is required to reset the neighbors to make it take effect.
- When configuring policy for neighbors in the incoming direction, you can configure multiple policies at the same time. For BGP, the following sequence applies: **distribute-list**, **filter-list**, **prefix-list**, and **route-map**. After the first policy is rejected, the following policy will not be implemented. Only after all the policies configured pass will the route be added to the database.
- For the routing policies applied in the incoming direction of BGP, the match options supported include as-path, community, extcommunity, ip address, ip nexthop, and metric, and the set options supported include as-path, comm-list, community, extcommunity, ip next-hop, local-preference, metric, origin, and weight.

## Configure the Maximum Number of Routing Entries Received by BGP Neighbors

For BGP device, you can limit the number of routing entries received from the designated neighbor. It gives alarms or disconnects when the routes received from the designated neighbor reaches a certain threshold.

Table 5 Configuring Maximum Number of Routing Entries Received by BGP Neighbors

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Configure the maximum number of routing entries received by neighbors	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>maximum-prefix</b> <i>prefix-num</i> [ <i>threshold-value</i> ] [ <b>warning-only</b> ]	Mandatory By default, the number of prefix entries received from neighbors is not restricted.

### Note

- If the warning-only command option is not specified, the BGP session will be automatically disconnected when the number of routing entries received by BGP from the neighbor reaches the maximum.
- If the warning-only command option is specified, when the number of routing entries received by BGP from the neighbor reaches the maximum, only alarm message is given, and route learning continues.

### Configure the Maximum Number of BGP Load Balancing Entries

In the BGP networking environment, if there are several paths with the same cost to reach the same destination, you can achieve load balancing routing by configuring the number of BGP load entries.

Table 60 Configuring Maximum Number of Load Balancing Entries of BGP

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-

Step	Command	Description
Configure the maximum number of IBGP load entries	<b>maximum-paths ibgp</b> <i>number</i>	Mandatory By default, there is no load balancing routing for IBGP.
Configure the maximum number of EBGP load entries	<b>maximum-paths</b> <i>number</i>	Mandatory By default, there is no load balancing routing for EBGP.

---

### Note

- After configuring the maximum number of EBGP load balancing entries, load can be formed only when EBGP route is preferred.
  - The commands used to configure the maximum number of load balancing entries vary with BGP configuration modes. For details, see the description of **maximum-paths** in BGP technical manual.
- 

## 60.2.4 Configure BGP Route Attributes

### Configuration Condition

Before configuring BGP route attributes, ensure that:

- Enable BGP protocol;
- Configure BGP neighbor and successfully establish and connect a session.

### Configure BGP Route Weight

The first rule for BGP routing is to compare the value of route weight. The larger the value, the higher the priority. The value of route weight is a local attribute of the device. It will not be transmitted to other BGP neighbors. It ranges from 0 to 65535. By default, the weight value of route learned from neighbors is 0, and those of all the routes generated on local device are 32768.

Table 6 Configuring BGP Route Weight

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Configure the route weight of neighbor or peer group	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>weight</b> <i>weight-num</i>	Mandatory By default, the route weight of neighbor is 0.

### Configure MED Attributes of BGP Route

MED attributes can be used to select the optimal route for the traffic entering AS. When other routing conditions are the same, if BGP learns the routes with the same destination address yet different next hops from different EBGP neighbors, it prefers that with the minimum MED value as the optimal entrance.

Sometimes MED is also called "external metric". It is marked as "metric" in the routing table of BGP. BGP will advertise the MED attributes of the routes learned from neighbors to IBGP neighbors rather than EBGP neighbors. Thus, MED is only applicable between neighboring AS.

#### 1. Configure BGP to allow comparison of MEDs from different AS neighboring routes

By default, BGP only performs MED routing for the routes learned from the same AS. You can use the **bgp always-compare-med** command to ignore the restriction on the same AS in MED routing.

Table 7 Configuring BGP to Allow Comparison of MEDs from Different AS Neighboring Routes

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Configure BGP to allow comparison of MEDs from different AS neighboring routes	<b>bgp always-compare-med</b>	Mandatory By default, BGP only allows to compare MEDs of the routes from the same AS

#### 2. Configure BGP to prioritise MEDs according to the route AS\_PATH-based group

By default, BGP doesn't prioritise MEDs according to the route AS\_PATH-based group. You can enable this function using the command **bgp deterministic-med**. When selecting routes, all routes are arranged based on AS\_PATH. Within each AS\_PATH group, the routes are ranked according to the MED size. The route with the minimum MED value is selected as the best route of this group.

Table 8 Configuring BGP to Prioritise MEDs According to the Route AS\_PATH-based Group

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
BGP prioritises MEDs according to the route AS_PATH-based group	<b>bgp deterministic-med</b>	Mandatory By default, BGP doesn't prioritise MEDs according to the route AS_PATH-based group.

### 3. Configure to compare MEDs of local confederated routes

By default, EBGP routes from different AS don't compare MED attributes. This principle also applies to the confederated EBGP. The command **bgp bestpath med confed** is used to enable comparison of MED attribute values for local confederated routes.

Table 60 Configuring BGP to Compare MEDs of Local Confederated Routes

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Configure BGP to compare MEDs of local confederated routes	<b>bgp bestpath med confed</b>	Mandatory By default, the MEDs of local confederated routes are not compared.

#### 4. Configure the routing map to modify MED attributes

For route sending and receiving, routing map can be used to modify the value of MED attributes.

Table 9 Configuring Routing Map to Modify MED Attributes

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Configure the routing map to modify MED attributes	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>route-map</b> <i>rtmap-name</i> <b>in</b>   <b>out</b>	Mandatory By default, routing map is not applied to any neighbor.

#### Note

- When configuring the routing map to modify MED attributes, you are required to modify MED with the **set metric** command, see the policy tool-**set metric**.
- After the **neighbor attribute-unchanged** command is configured, MED attributes of the neighbor cannot be changed through routing map.

#### Configure Local-Preference Attributes of BGP Route

Local-Preference attributes are transmitted among IBGP neighbors only. Local-Preference is used to select the optimal exit to leave AS. The route with the largest route will be preferred.

Its value ranges from 0 to 4294967295. The larger the value, the higher the priority. By default, all the routes advertised to IBGP neighbors have a Local-Preference attribute of 100, which can be modified through **bgp default local-preference** or routing map.

##### 1. Configure BGP to modify default Local-Preference attributes

Table 10 Configuring BGP to Modify Default Local-Preference Attributes

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Configure the default Local-Preference value	<b>bgp default local-preference</b> <i>local-value</i>	Optional By default, the local preference is 100.

## 2. Configure the routing map to modify Local-Preference attributes

Table 11 Configuring Routing Map to Modify Local-Preference Attributes

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Configure the routing map to modify Local-Preference attributes	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>route-map</b> <i>rtmap-name</i> <b>in</b>   <b>out</b>	Mandatory By default, routing map is not applied to any neighbor.

### Note

- When configuring the routing map to modify Local-Preference attributes, you are required to modify Local-Preference attributes with the **set local-preference** command, see the policy tool-set **local-preference**.

## Configure AS\_PATH Attributes of BGP Route

### 1. Configure BGP to ignore comparison of AS\_PATH in routing

When other conditions are the same, BGP will prefer the route with the shortest AS\_PATH. You can cancel AS\_PATH routing via the command **bgp bestpath as-path ignore**.

Table 12 Configuring BGP to Ignore Comparison of AS\_PATH in Routing

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Configure BGP to ignore comparison of AS_PATH in routing	<b>bgp bestpath as-path ignore</b>	Mandatory By default, AS_PATH values are compared in routing.

## 2. Configure BGP for allowed Times of Repeated Local AS Number

In order to avoid routing loops, BGP will check the AS\_PATH attributes of the routes received from neighbors, and discard those containing local AS number. You may use the command **neighbor allowas-in** to allow the routes received by BGP to contain local AS number, and can configure the number of local AS numbers.

Table 13 Configuring BGP for allowed Times of Repeated Local AS Number

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Configure to allow repeated local AS number	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>allowas-in</b> [ <i>as-num</i> ]	Mandatory By default, the AS_PATH attributes of the routes received from neighbors are not allowed to contain local AS number.

## 3. Configure BGP to remove private AS number when advertising route to neighbors

In large BGP networks, the AS\_PATH of routing has the following attributes: confederation or community. By default, BGP carries these private AS attributes when advertising to neighbors. In order to shield private network information, you can use **neighbor remove-private-AS** to remove private AS number.

Table 14 Configuring BGP to Remove Private AS Number When Advertising Route to Neighbors

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Configure BGP to remove private AS number when advertising route to neighbors	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>remove-private-AS</b>	Mandatory By default, private AS number is carried when advertising to neighbors.

#### 4. Configure to detect legality of first AS number of EBGp route

When BGP advertises route to EBGp neighbors, the local AS number is pressed to the start position of AS\_PATH, and the first AS advertising this route will become the last one. Generally, the first AS number of the route received from EBGp should be the same as the AS number of neighbors. Otherwise, this route will be discarded.

Table 15 Configuring to Detect Legality of First AS Number of EBGp Route

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Configure to detect legality of the first AS number of EBGp route	<b>bgp enforce-first-as</b>	Mandatory By default, the first AS number check mechanism is disabled in BGP.

#### 5. Configure the routing map to modify AS\_PATH attributes

BGP supports the configuration of routing map to modify AS\_PATH attributes. You can add route attributes via **set as-path prepend** so as to affect the routing of neighbors. When using the function **set as-path**

**prepend**, local AS is first used to add AS\_PATH. When using other AS, enough attention must be paid to avoid being rejected in route advertisement to this AS.

Table 16 Configuring Routing Map to Modify AS\_PATH Attributes

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Configure the routing map to modify AS_PATH attributes	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>route-map</b> <i>rtmap-name</i> <b>in</b>   <b>out</b>	Mandatory By default, routing map is not applied to any neighbor.

### Note

- When configuring the routing map to modify AS\_PATH attributes, you are required to modify AS\_PATH attributes with the **set as-path prepend** command, see the policy tool-**set as-path**.

### Configure NEXT-HOP Attributes of BGP Route

When BGP advertises routes to IBGP neighbors, the route attributes (including next hop) are not changed. The next hop attribute is often used for BGP to advertise the routes learned by EBGP neighbors to IBGP neighbors. The **neighbor next-hop-self** command can be used to modify the next hop attribute of the routes advertised to BGP neighbors to use local IP address. For BGP, you can also use routing map to modify the next hop attribute.

#### 1. Configure BGP to use local IP address as next hop of route

Table 17 Configuring BGP to Use Local IP Address as Next Hop of Route

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-

Step	Command	Description
Configure to use local IP address as the next hop when advertising routes to neighbors	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>next-hop-self</b>	Mandatory  By default, the next hop attribute of the route advertised to EBGp neighbor is local IP address. The next hop attribute of the route advertised to IBGP will not be modified. Its original attribute value will be kept unchanged.

### Note

- When configuring BGP to use local IP address as the next hop of the route, if the source address of the TCP session is configured with the **neighbor update-source**, it will be used as the next hop address. Otherwise, the output interface IP of the advertising device will be selected as local IP address.

## 2. Configure the routing map to modify NEXT-HOP attributes

BGP supports the configuration of routing map to modify NEXT-HOP attributes through **set ip next-hop**.

Table 18 Configuring Routing Map to Modify NEXT-HOP Attributes

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Configure the routing map to modify NEXT-HOP attributes	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>route-map</b> <i>rtmap-name</i> <b>in</b>   <b>out</b>	Mandatory  By default, routing map is not applied to any neighbor.

---

## Note

- When configuring the routing map to modify NEXT-HOP attributes, you are required to modify NEXT-HOP attributes with the **set ip next-hop** command, see the policy tool-**set ip next-hop**.
- 

### Configure Community Attributes of BGP Route

When advertising routes to neighbors, BGP allows the configuration of sending community attributes. You can apply routing map to match community attributes for specified neighbors in both incoming and outgoing directions.

Community attributes are used to identify a group of routes so as to apply routing policy to them. Community attributes have two forms, i.e. standard and extended. Standard community attributes have 4 bytes. Their attributes include NO\_EXPORT, LOCAL\_AS, NO\_ADVERTISE, and INTERNET. Extcommunity attributes have 8 bytes. Their attributes include Route Target (RT) and Route Origin.

#### 1. Configure BGP to advertise community attributes of route to neighbors

**neighbor send-community** allows to advertise standard or extcommunity attributes or both to neighbors.

Table 19 Configuring BGP to Advertise Community Attributes of Route to Neighbors

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Configure to advertise community attributes of route to neighbors	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>send-community</b> [ <b>both</b>   <b>extended</b>   <b>standard</b> ]	Mandatory By default, community attributes are not advertised to any neighbor.

---

## Note

- After the neighbor is activated under VPNv4 address family, the standard and extcommunity attributes will be automatically advertised to neighbors.
-

## 2. Configure the routing map to modify community attributes of route

BGP supports the configuration of routing map to modify community attributes through **set communtiy**.

Table 60 Configuring Routing Map to Modify Community Attributes of Route

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Configure the routing map to modify community attributes of BGP route	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>route-map</b> <i>rtmap-name</i> <b>in</b>   <b>out</b>	Mandatory By default, routing map is not applied to any neighbor.

---

### Note

- When configuring the routing map to modify community attributes of the route, you are required to modify community attributes with the **set communtiy** command, see the policy tool-**set communtiy**.
- 

## 60.2.5 Configure BGP Network Optimization

### Configuration Condition

Before configuring BGP network optimization, ensure that:

- Enable BGP protocol;
- Configure BGP neighbor and successfully establish and connect a session.

### Configure Keepalive Time of BGP Neighbor

After a BGP session is successfully established, neighbors will periodically send Keepalive messages to maintain the BGP session relationship. If the neighbor's Keepalive message or route update packet is not received within the holdtime, the BGP session will be disconnected for over time. The keepalive time of the session will not be more than one third of the holdtime.

Table 20 Configuring Keepalive Time of BGP Neighbor

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Configure keepalive time and holdtime of global BGP	<b>timers bgp</b> <i>keepalive-interval holdtime-interval</i>	Optional
Configure the keepalive time and holdtime of BGP neighbor or peer group	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>timers</b> { <i>keepalive-interval holdtime-interval</i>   <b>connect</b> <i>connect-interval</i> }	By default, the interval of keepalive timer is 60 seconds; the interval of hold timer is 180 seconds; the interval of session reconnection timer is 120 seconds.

## Note

- The keepalive time and holdtime configured for specified neighbors precede those of global BGP.
- After neighbor negotiation, the minimum holdtime will be used as the holdtime of BGP session.
- When both keepalive time and holdtime are configured as zero, the neighbor keepalive/hold function is cancelled.
- When the keepalive time interval is more than one third of the holdtime, the BGP session sends keepalive packets within one third of the holdtime.

### Configure BGP Route Detection Time

BGP mainly completes the pathfinding process with AS as the unit, and IGP completes the pathfinding process within the AS. Therefore, BGP routing often relies on IGP routing. After the next hop or output interface of IGP route on which BGP relies changes, BGP updates BGP route by periodically detecting IGP route. Update of local BGP route and other matters are completed within the detection period.

Table 21 Configuring BGP Route Detection Time

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Configure BGP Route Detection Time	<b>bgp scan-time</b> <i>time</i>	Optional By default, the BGP route detection time is 60 seconds.

## Caution

- When a very short BGP route detection time is configured, BGP will frequently detect routes. This will affect the performance of the device.

### Configure Fast Disconnection of EBGP Neighbor

After a BGP session is successfully established, neighbors will periodically send Keepalive messages to each other to maintain the BGP session relationship. If the neighbor's Keepalive message or route update packet is not received within the holdtime, the BGP session will be disconnected for over time. You can configure a direct EBGP neighbor to disconnect BGP connection immediately when the connected interface is down, without waiting for the BGP keepalive timeout. When the fast disconnection of EBGP neighbors is cancelled, the EBGP session will not give a response to the down event on the interface. It will be disconnected after timeout.

Table 22 Configuring Fast Disconnection of EBGP Neighbor

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Configure Fast Disconnection of EBGP Neighbor	<b>bgp fast-external-failover</b>	Optional By default, EBGP can give a fast response to the offline event on the direct interface.

### Configure BGP Route Dampening Function

Frequent route flapping in the network will make the network unstable. BGP suppresses such routes by configuring route dampening to reduce the impact of route flapping on the network.

For the routes subject to frequent flapping, their penalty value will increase. When the penalty value exceeds the dampening threshold, the route will not be advertised to neighbors. The penalty value shall not exceed the maximum dampening time. When no route flapping happens during the half-life, the penalty value will be halved. The route will not be re-advertised to neighbors until the value is less than the reuse limit.

- Half-life: The period when the penalty value of route is halved.
- Reuse limit: The limit that route returns to service.
- Suppress limit: The limit that the route is suppressed.
- Max suppress time: The maximum time that the route is suppressed.

Table 23 Configuring BGP Route Suppression Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Configure BGP route dampening period	<b>bgp dampening</b> [ <i>reach-half-life</i> [ <i>reuse-value</i> <i>suppress-value</i> <i>max-suppress-time</i> [ <i>unreach-half-life</i> ] ] ]   <b>route-map</b> <i>rtmap-name</i> ]	Mandatory  By default, the route suppression function is disabled. After it is enabled, the default route suppression half-life is 15 minutes; the route reuse limit is 750; the route suppress limit is 2000; the max suppress time is 60 minutes; the unreachable half-life of route penalty is 15 minutes.

 **Note**

- Route flapping includes both addition or deletion of routes, and change of route attributes,

---

such as next hop and MED attributes.

---

### Configure BGP Neighbor Refresh Capability

When the routing policy or route selection policy applied by BGP neighbors changes, the routing table needs to be refreshed again by two manners. One is to reset by recovering BGP connection to restart the session. This method may cause BGP route flapping and affect business operation. The other one is more graceful. You need to configure the BGP device of local port to support the capability of route refresh. When its neighbor needs to reset the route, the Route-Refresh message is sent to local port which will re-send the route to this neighbor after receiving the message. In this case, the routing table is dynamically refreshed without disconnecting BPG sessions.

Table 24 Configuring Refreshing Capability of BGP Neighbor

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Enable BGP Neighbor Refresh Capability	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>capability route-refresh</b>	Optional By default, advertising neighbors to support route refresh capability is enabled.

### Configure Soft Resetting Capability of BGP Neighbor

When the routing policy or route selection policy applied by BGP neighbors changes, the routing table needs to be refreshed again by two manners. One is to reset by recovering BGP connection to restart the session. This method may cause BGP route flapping and affect business operation. Another more graceful method is to configure local BGP device to support route refresh capability. You can also enable the soft resetting capability of local BGP device. By default, the BGP device retains the routing information of all neighbors. After enabling its neighbors' soft reset capability, it refreshes the routes of local retained neighbors again. At this time, the BGP session will not be disconnected.

Table 25 Configuring Soft Resetting Capability of BGP Neighbor

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Enable soft resetting capability of BGP neighbor	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>soft-reconfiguration inbound</b>	Mandatory By default, the soft resetting function is disabled.

### Configure ORF Capability of BGP Neighbor

BGP accurately controls routes through various route attributes. To this end, it usually applies routing policy in both incoming and outgoing directions, a local behavior of BGP. BGP also supports ORF (Outbound Route Filtering) capability. It advertises local ingress policy through Route-refresh packet to its neighbor which applies this policy when advertising routes to it. This can largely reduce the interactions of route update packet between BGP neighbors.

To successfully negotiate ORF capability, the following conditions must be satisfied:

- Both neighbors need to enable ORF capability;
- ORF send and ORF receive must be paired, i.e., if one uses ORF send, the other must be ORF both or ORF receive; if one uses ORF receive, the other must be ORF send or ORF both;
- For the neighbor using ORF send, a prefix list needs to be applied in the incoming direction.

Table 26 Configuring ORF Capability of BGP Neighbor

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-

Step	Command	Description
Make the neighbor apply prefix list in the incoming direction	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>prefix-list</b> <i>prefix-list-name</i> <b>in</b>	Mandatory By default, prefix list is not applied to any BGP neighbor.
Make the neighbor support ORF capability	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>capability orf prefix-list</b> { <b>both</b>   <b>receive</b>   <b>send</b> }	Mandatory By default, advertising neighbors to support ORF capability is disabled.

## 60.2.6 Configure Large BGP Network

### Configuration Condition

Before configuring large BGP network, ensure that:

- Enable BGP protocol;
- Configure BGP neighbor and successfully establish and connect a session.

### Configure BGP Peer Group

BGP peer group is a set of BGP neighbors with the same configuration policy. Any configuration of the peer group will influence all the members in the group. Configuring BGP peer group is beneficial for the centralized management and maintenance of neighbors.

Table 27 Configuring BGP Peer Group

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Create BGP peer group	<b>neighbor</b> <i>peer-group-name</i> <b>peer-group</b>	Mandatory By default, peer group is not configured, and neighbors are not added into any peer group.
Add neighbors into the peer group	<b>neighbor</b> <i>neighbor-address</i> <b>peer-group</b> <i>peer-group-name</i>	

---

 **Note**

- The configuration of peer group will influence all the group members.
  - After a neighbor is added into the peer group, the configuration of the original one which is the same as that of the peer group will be deleted.
  - After configuring the routing policy in outgoing and incoming directions for the peer group, if the routing policy changes, it is not effective for the neighbor already added into the peer group. The altered routing policy cannot apply to members of the peer group until the peer group is reset.
- 

### Configure BGP Route Reflector

In large BGP networking environments, IBGP neighbors are required to be connected across the whole network. That is to say, each BGP has to connect with all the other IBGP neighbors. Then, in the networking environment with N BGP neighbors, there are  $N*(N-1)/2$  BGP connections. The more the connections, the larger the amount of route advertisement. BGP route reflector can reduce the number of network connections. It includes several IBGPs into a group, and specifies a BGP as a reflector (RR), other BGPs as clients, and the BGPs not in the group as non-clients. The clients establish peering relationships with the PR only to reduce necessary IBGP connections. The number of connections can be decreased to N-1.

The principle of reflecting routes by BGP route reflector:

- The routes learned from non-client IBGP neighbors are reflected to clients only;
- The routes learned from clients will be reflected to all the clients and non-clients except the clients initiating these routes;
- The routes learned from EBGPs will be reflected to all the clients and non-clients.

Table 28 Configuring BGP Route Reflector

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Configure reflector cluster ID	<b>bgp cluster-id</b> { <i>cluster-id-in-ip</i>   <i>cluster-id-in-num</i> }	Mandatory By default, the route reflector cluster ID is the Router ID of the device.

Step	Command	Description
Configure neighbor as reflector client	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>route-reflector-client</b>	Mandatory By default, no neighbor is specified as reflector client.
Configure the route reflection function between BGP clients	<b>bgp client-to-client reflection</b>	Optional By default, the route reflection function between BGP route reflector clients is enabled.

### Note

- Reflector cluster ID is used to identify the same reflector area with many reflectors that have the same reflector cluster ID.

## Configure BGP Confederation

In large BGP networking environments, IBGP neighbors are required to be connected across the whole network. That is to say, each BGP has to connect with all the other IBGP neighbors. Then, in the networking environment with N BGP neighbors, there are  $N*(N-1)/2$  BGP connections. The more the connections, the larger the amount of route advertisement. BGP confederation can also reduce network connections. It uses the divide-and-conquer strategy to divide the AS into several sub-AS areas. Each of them forms a confederation which is fully connected through IBGP. The sub-AS areas of the confederation are connected via EBGp to effectively reduce BGP connections.

When configuring BGP confederation, it is required to assign a confederation ID to each confederation and specify members of such confederation. Unlike route reflector (only route reflector is required to support route reflection when necessary), confederation requires all members to support the confederation function.

Table 29 Configuring BGP Confederation

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Create BGP confederation ID	<b>bgp confederation identifier</b> <i>as-number</i>	Mandatory By default, no confederation AS number is configured.
Configure BGP confederation members	<b>bgp confederation peers</b> <i>as-number-list</i>	Mandatory By default, the confederation's sub-AS number is not configured.

---

### Note

- The confederation ID is used to identify the confederation sub-AS which contains the confederation members.
- 

## 60.2.7 Configure BGP GR

GR (Graceful Restart) is used to keep the routing information in the forwarding layer of this device and neighbor device unchanged during the switch between host and standby devices to ensure the forwarding process is not affected; after the device is switched for re-running, the two devices synchronize routing information and update forwarding layer in the protocol layer so that the data can keep forwarding during the process of device switch.

Roles in GR process:

- GR Restarter: The device for graceful restart of protocol;
- GR Helper: The device which helps with the graceful restart of protocol;
- GR Time: The maximum time for GR-Restarter to restart. GR Helper maintains routing stability during this period of time only.

The dual-master device can act as GR Restarter and GR Helper, while the centralized device only serves as GR Helper to help the Restarter complete GR. When the GR Restarter is doing GR, GR Helper maintains its route until GR Time is time out and the GR is completed for routing information synchronization. During

this period of time, network routing and packet forwarding stays at the status prior to GR, which effectively ensures network stability.

BGP GR relationship is established through OPEN packet negotiation when neighbors establish connections. When the GR Restarter neighbor restarts, the BGP session will be disconnected, but the routes learned from the neighbor will not be deleted. They will continue to be forwarded normally in the IP routing table. Marked with Stale in the BGP routing table, they will be updated after GR is completed or time out.

GR Restarter needs to complete the connection with GR Helper within the maximum allowable time. Otherwise, GR Helper will eliminate the GR routes retained and cancel the GR process. After neighbor re-establishment is completed, the GR Helper needs to receive the update packets with End-Of-RIB tag from the GR Restarter to successfully complete the GR process. Otherwise, the GR route not updated will be deleted after the maximum hold time (**stalepath-time**), and the GR relationship will be cancelled.

### Configuration Condition

Before configuring BGP GR, ensure that:

- Enable BGP protocol;
- Configure BGP neighbor and successfully establish and connect a session.

### Configure BGP GR Restarter

Table 30 Configuring BGP GR Restarter

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Enable BGP GR capability	<b>bgp graceful-restart</b> [ <b>restart-time</b> <i>time</i>   <b>stalepath-time</b> <i>time</i> ]	Mandatory  By default, the GR capability is not enabled on the BGP device. After GR is enabled, the default maximum allowable time for neighbors to re-establish sessions is 120 seconds; the maximum hold time of GR routes is 360 seconds.

Step	Command	Description
Configure to advertise GR-Restarter capability to neighbors	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>capability graceful-restart</b>	Mandatory By default, GR-Restarter capability is not advertised to any neighbor.

### Configure BGP GR Helper

Table 31 Configuring BGP GR Helper

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Enable BGP GR capability	<b>bgp graceful-restart</b> [ <b>restart-time</b> <i>time</i>   <b>stalepath-time</b> <i>time</i> ]	Mandatory By default, the GR capability is not enabled on the BGP device. After GR is enabled, the default maximum allowable time for neighbors to re-establish sessions is 120 seconds; the maximum hold time of GR routes is 360 seconds.

### 60.2.8 Configure BGP to Coordinate with BFD

Generally, there are other intermediate devices between BGP neighbors. When these devices fail, BGP sessions are normal within the hold time. They cannot give a response to the link failures of intermediate devices in a timely manner. BFD (Bidirectional Forwarding Detection) provides a method to quickly detect the status of lines between two devices. When BFD detection is enabled between BGP devices, if there is a line failure between the devices, BFD can quickly detect the failure and notify BGP to trigger BGP to rapidly disconnect the session and switch to the backup line. In this way, it can reach the purpose of fast route switch.

## Configuration Condition

Before configuring the coordination of BGP with BFD, ensure that:

- Enable BGP protocol;
- Configure BGP neighbor and successfully establish and connect a session.

## Configure EBGP to Coordinate with BFD

The coordination of EBGP with BFD is based on single-hop BFD sessions, and BFD session parameters are required to be configured in interface mode.

Table 60 Configuring Coordination of EBGP with BFD

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Configure EBGP to Coordinate with BFD	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>fall-over bfd</b>	Mandatory By default, the BFD function of neighbor is disabled.
Exit the BGP configuration mode	<b>exit</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure the minimum receiving time interval of BFD sessions	<b>bfd min-receive-interval</b> <i>milliseconds</i>	Optional By default, the minimum receiving time interval of BFD sessions is 1000 milliseconds.
Configure the minimum sending time interval of BFD sessions	<b>bfd min-transmit-interval</b> <i>milliseconds</i>	Optional By default, the minimum sending time interval of BFD sessions is 1000 milliseconds.

Step	Command	Description
Configure the BFD session detection timeout multiple	<b>bfd multiplier</b> <i>number</i>	Optional The BFD session detection timeout multiple is 5.

## Note

- For the BFD-related configurations, please see the Reliability Technology - BFD-related section.

## 60.2.9 Configure BGP FRR

### Configuration Condition

Before configuring the coordination of BGP with BFD, ensure that:

- Enable BGP protocol.
- Configure BGP neighbor and successfully establish and connect a session.

### Configure BGP FRR

In the BGP network, as a result of link or device failure, the packets passing the point of failure will be discarded or loops will be produced. The traffic interruption caused thereby will continue until the protocol reconverges after several seconds. BGP FRR can reduce the time of traffic interruption. By applying the routing map, set a backup next hop for the successfully matched route. Once the main link fails, the traffic passing through the main link will immediately switch to the backup link, achieving the purpose of fast switching.

Table 32 Configuring BGP FRR

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Configure BGP FRR	<b>fast-reroute route-map</b> <i>rtmap-name</i>	Optional By default, the FRR function is disabled.

Configure BGP auto FRR	<b>pic</b>	Mandatory By default, the BGP auto FRR function is disabled.
------------------------	------------	---

## Caution

- After BGP FRR is configured, BGP needs to be reset to complete initial route check and backup. Otherwise, it is only effective for the routes learned after the configuration.
- When set fast-reroute backup-nexthop auto is configured for the FRR based on route-map, the protocol enables automatic FRR;
- When pic method is used, the protocol enables automatic FRR;
- The methods of enabling FRR are mutually exclusive;
- After configuring BGP FRR and applying the routing map, use the command **set fast-reroute backup-nexthop** *nexthop-address* to set the BGP neighbor as the backup next hop in the routing map. If the non-BGP neighbor is configured as the backup next hop, the FRR function cannot take effect.

## 60.2.10 Configure BGP LS

### Configuration Condition

Before configuring BGP LS, ensure that:

- Enable OSPF protocol.
- Establish neighbors for OSPF and configure distribute link-state.

### Configure BGP LS

Configure BGP LS to collect the topological information of IGP protocol.

Table 60-33 Configuring BGP LS

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-

Configure BGP link-state address family	<b>address-family link-state unicast</b>	Optional By default, the link-state address family is disabled.
Activate the LS capability of BGP neighbor	<b>neighbor { neighbor-address   peer-group-name } activate</b>	Optional By default, the LS capability of BGP neighbor is not activated.

## 60.2.11 BGP monitoring and maintaining

Table 34 BGP Monitoring and Maintaining

Command	Description
<b>clear ip bgp</b> { *   <i>neighbor-address</i>   <i>as-number</i>   <b>peer-group</b> <i>peer-group-name</i>   <b>external</b> } [ <b>vrf</b> <i>vrf-name</i>   <b>ipv4 unicast</b>   <b>ipv4 multicast</b>   <b>vpn4 unicast</b>   <b>mvpn</b> ]	Reset BGP neighbors
<b>clear ip bgp</b> [ <b>ipv4 unicast</b>   <b>ipv4 multicast</b> ] <b>dampening</b> [ <i>ip-address</i>   <i>ip-address/mask-length</i> ]	Clear dampened routes
<b>clear ip bgp</b> [ <b>ipv4 unicast</b>   <b>ipv4 multicast</b> ] <b>flap-statistics</b> [ <i>ip-address</i>   <i>ip-address/mask-length</i> ]	Clear jitter statistics
<b>clear ip bgp</b> { *   <i>neighbor-address</i>   <i>as-number</i>   <b>peer-group</b> <i>peer-group-name</i>   <b>external</b> } [ <b>ipv4 unicast</b>   <b>ipv4 multicast</b>   <b>vpn4 unicast</b>   <b>vrf</b> <i>vrf-name</i>   <b>mvpn</b> ] { [ <b>soft</b> ] [ <b>in</b>   <b>out</b> ] }	Softly reset neighbors
<b>clear ip bgp</b> { *   <i>neighbor-address</i> } <b>in</b> { <b>ecomm</b>   <b>prefix-filter</b> }	Advertise ORF to neighbors
<b>show ip bgp</b> [ <b>vpn4</b> { <b>all</b>   <b>vrf</b> <i>vrf-name</i>   <b>rd</b> <i>route-distinguisher</i> } ] [ <i>ip-address</i>   <i>ip-address/mask-length</i> ]	Show the routing information under corresponding address family of BGP

Command	Description
<b>show ip bgp attribute-info</b>	Show the public route attributes of BGP
<b>show ip bgp cidr-only</b>	Show all classful network routes of BGP
<b>show ip bgp community</b> [ <i>community-number</i> / <i>aa:nn</i> / <b>exact-match</b> / <b>local-AS</b> / <b>no-advertise</b> / <b>no-export</b> ]	Show the routing information which matches specified community attributes
<b>show ip bgp community-info</b>	Show the community attributes of all BGP
<b>show ip bgp community-list</b> <i>community-list-name</i>	Show the community attribute list applied to routing information
<b>show ip bgp</b> [ <b>vpn4</b> { <b>all</b>   <b>vrf</b> <i>vrf-name</i>   <b>rd</b> <i>route-distinguisher</i> } ] <b>dampening</b> { <b>dampened-paths</b>   <b>flap-statistics</b>   <b>parameters</b> }	Show detailed information of route dampening
<b>show ip bgp filter-list</b> <i>filter-list-name</i> [ <b>exact-match</b> ]	Show the routes matching AS_PATH access list
<b>show ip bgp inconsistent-a</b>	Show the routes in conflict with AS_PATH
<b>show ip bgp ipv4 vpn-target</b> [ <i>vpn-rt</i> ]	Show the VPN-TARGET routing table of BGP
<b>show ip bgp ipv4 vpn-target rt-filter</b> [ <b>neighbor</b> <i>ip-address</i> ]	Show the RT filter list of BGP neighbors
<b>show ip bgp mvpn</b> { <b>all</b>   <b>vrf</b> <i>vrf-name</i>   <b>rd</b> <i>route-distinguisher</i> } { <b>all-type</b>   <b>type</b> { <b>1</b> [ <i>ip-address</i> ]   <b>7</b> [ <i>as:source-ip-address:group-ip-address</i> ] } }	Show the routing information under MVPN address family of BGP
<b>show ip bgp mvpn</b> { <b>all</b>   <b>vrf</b> <i>vrf-name</i>   <b>rd</b> <i>route-distinguisher</i> } { <b>neighbors</b> <i>ip-address</i> } { <b>advertised-routes</b>   <b>received-routes</b>   <b>routes</b> } { <b>all-type</b>   <b>type</b> { <b>1</b> [ <i>ip-address</i> ]   <b>7</b> [ <i>as:source-ip-address:group-ip-address</i> ] } }	Show the routing information of specified neighbors under MVPN address family of BGP
<b>show ip bgp mvpn</b> { <b>all</b>   <b>vrf</b> <i>vrf-name</i>   <b>rd</b> <i>route-distinguisher</i> / <b>neighbors</b> <i>ip-address</i> } { <b>all-type</b>   <b>type</b> { <b>1</b>   <b>7</b> } } { <b>statistics</b> }	Show the statistical information of the routes under MVPN address family of BGP

Command	Description
<b>show ip bgp</b> [ <b>vpn4</b> { <b>all</b>   <b>vrf</b> <i>vrf_name</i>   <b>rd</b> <i>route-distinguisher</i> } ] <b>neighbors</b> [ <i>ip-address</i> ]	Show the detailed information BGP neighbors
<b>show ip bgp orf ecomm</b>	Show the ORF information of all BGP neighbors
<b>show ip bgp paths</b>	Configure the AS_PATH information of BGP routes
<b>show ip bgp prefix-list</b> <i>prefix-list-name</i>	Show the routes matching prefix list
<b>show ip bgp quote-regexp</b> <i>as-path-list-name</i>	Show the routes matching AS_PATH list
<b>show ip bgp regexp</b> <i>as-path-list-name</i>	Show the routes matching AS_PATH list
<b>show ip bgp route-map</b> <i>rtmap-name</i>	Show the route matching the routing map
<b>show ip bgp scan</b>	Show the scanning information of BGP
<b>show ip bgp</b> [ <b>vpn4</b> { <b>all</b>   <b>vrf</b> <i>vrf-name</i>   <b>rd</b> <i>route-distinguisher</i> }   <b>mvpn</b> ] <b>summary</b>	Show the neighbor summarization information of BGP

## 60.3 Typical configuration example of BGP

### 60.3.1 Configure basic functions of BGP

#### Network Requirements

- EBGP neighbors are established between Device1 and Device2, and IBGP neighbors are established between Device2 and Device3.
- Device1 learns the direct route 200.0.0.0/24 from the interface of Device3 which learns the direct route 100.0.0.0/24 from the interface of Device1.

#### Network Topology

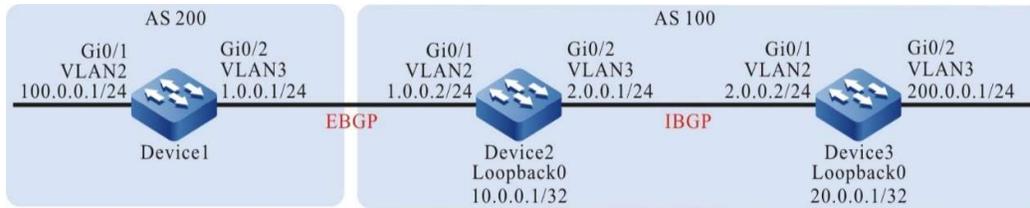


Figure 60 Network Topology for Configuring Basic Functions of BGP

### Configuration Steps

- Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)
- Step 2: Configure IP addresses for the ports. (Omitted)
- Step 3: Configure OSPF so that the routes of Loopback between devices are reachable from each other.

#### #Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 10.0.0.1 0.0.0.0 area 0
Device2(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#exit
```

#### #Configure Device3.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#network 20.0.0.1 0.0.0.0 area 0
Device3(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#exit
```

#### #View the routing table of Device 2.

```
Device2#show ip route ospf
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
U - Per-user Static route
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

O 20.0.0.1/32 [110/2] via 2.0.0.2, 00:27:09, vlan3
```

#### #Check the routing table of Device3.

```
Device3#show ip route ospf
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
U - Per-user Static route
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

O 10.0.0.1/32 [110/2] via 2.0.0.1, 00:28:13, vlan2
```

According to the result, both Device2 and Device3 have learned the route of peer loopback interface by running OSPF protocol. On this basis, Device2 and Device3 can establish IBGP neighbors through loopback interface.

- Step 4: Configure BGP.

### #Configure Device1.

Establish a direct EBGP peer with Device2, and import 100.0.0.0/24 into BGP through the network.

```
Device1#configure terminal
Device1(config)#router bgp 200
Device1(config-bgp)#neighbor 1.0.0.2 remote-as 100
Device1(config-bgp)#network 100.0.0.0 255.255.255.0
Device1(config-bgp)#exit
```

### #Configure Device2.

Build indirect IBGP peer relationship with Device3 through Loopback0, and set the next hop of the advertised route as itself to establish a direct EBGP peer with Device1.

```
Device2(config)#router bgp 100
Device2(config-bgp)#neighbor 20.0.0.1 remote-as 100
Device2(config-bgp)#neighbor 20.0.0.1 update-source loopback0
Device2(config-bgp)#neighbor 1.0.0.1 remote-as 200
Device2(config-bgp)#neighbor 20.0.0.1 next-hop-self
Device2(config-bgp)#exit
```

### #Configure Device3.

Build indirect IBGP peer relationship with Device2 through Loopback0, and import 200.0.0.0/24 into BGP through the network.

```
Device3(config)#router bgp 100
Device3(config-bgp)#neighbor 10.0.0.1 remote-as 100
Device3(config-bgp)#neighbor 10.0.0.1 update-source loopback0
Device3(config-bgp)#network 200.0.0.0 255.255.255.0
Device3(config-bgp)#exit
```

---

## Note

- In order to avoid route flapping, IBGP neighbors are established through loopback interfaces. OSPF is required to synchronize the routing information of the loopback interfaces between IBGP neighbors.
- 

Step 5: Check the result.

#View the status of BGP neighbors on Device 2.

```
Device2#show ip bgp summary
BGP router identifier 10.0.0.1, local AS number 100
BGP table version is 2
2 BGP AS-PATH entries
0 BGP community entries

Neighbor    V  AS  MsgRcvd  MsgSent  TblVer  InQ  OutQ  Up/Down  State/PfxRcd
1.0.0.1     4  200    3      3        1    0  0 00:00:29  1
20.0.0.1    4  100    5      4        2    0  0 00:02:13  1
```

From the case where the content of the State/PfxRcd column is displayed as a digit (from the number of routing prefixes received by the neighbor), you can see that Device 2 has successfully established BGP neighbors with Device1 and Device3.

#View the routing table of Device1.

```
Device1#show ip route bgp
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

B 200.0.0.0/24 [20/0] via 1.0.0.2, 00:15:52, vlan3
```

#View the routing table of Device 2.

```
Device2#show ip route bgp
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

B 100.0.0.0/24 [20/0] via 1.0.0.1, 00:14:11, vlan2
B 200.0.0.0/24 [200/0] via 20.0.0.1, 00:17:12, vlan3
```

#Check the routing table of Device3.

```
Device3#show ip route bgp
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

B 100.0.0.0/24 [200/0] via 10.0.0.1, 00:14:50, vlan2
```

According to the result, Device1 learns the direct route 200.0.0.0/24 from the interface of Device3 which learns the direct route 100.0.0.0/24 from the interface of Device1.

## 60.3.2 Configure BGP Route Redistribution

### Network Requirements

- Device3 establishes OSPF neighbors with Device2, and advertises the direct route of the interface 200.0.0.0/24 to Device2.
- Establish EBGP neighbors between Device1 and Device2 so that Device2 will redistribute the OSPF route to BGP and advertise it to Device1.

### Network Topology

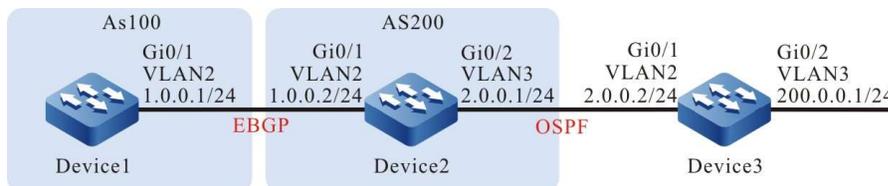


Figure 60 Network Topology for Configuring BGP Route Redistribution

### Configuration Steps

Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configure IP addresses for the ports. (Omitted)

Step 3: Configure OSPF so that the routes of Loopback between devices are reachable from each other.

#Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#exit
```

#Configure Device3.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#network 200.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#exit
```

#View the routing table of Device 2.

```
Device2#show ip route ospf
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
U - Per-user Static route
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

O 200.0.0.0/24 [110/2] via 2.0.0.2, 00:01:45, vlan3
```

It can be seen from the routing table that Device2 learns the OSPF route 200.0.0.0/24 advertised by Device3.

Step 4: Configure BGP.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#router bgp 200
Device1(config-bgp)#neighbor 1.0.0.2 remote-as 100
Device1(config-bgp)#exit
```

#Configure Device2.

```
Device2(config)#router bgp 100
Device2(config-bgp)#neighbor 1.0.0.1 remote-as 200
Device2(config-bgp)#exit
```

#View the status of BGP neighbors on Device 2.

```
Device2#show ip bgp summary
BGP router identifier 2.0.0.1, local AS number 100
BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries

Neighbor    V  AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State/PfxRcd
1.0.0.1    4  200    2     2     2  0  0 00:00:42    0
```

#It can be seen that BGP neighbors have been successfully established between Device 2 and Device1.

Step 5: Configure BGP to redistribute OSPF routes.

#Configure Device2.

```
Device2(config)#router bgp 100
Device2(config-bgp)#redistribute ospf 100
Device2(config-bgp)#exit
```

Step 6: Check the result.

#View the BGP routing table of Device2.

```
Device2#show ip bgp
BGP table version is 6, local router ID is 2.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop        Metric LocPrf Weight Path
[O]*> 2.0.0.0/24  0.0.0.0          1   32768 ?
[O]*> 200.0.0.0/24 2.0.0.2          2   32768 ?
```

According to the result, OSPF route has been successfully redistributed to BGP.

#View the routing table of Device1.

```
Device1#show ip route bgp
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

B 2.0.0.0/24 [20/1] via 1.0.0.2, 00:06:14, vlan2
B 200.0.0.0/24 [20/2] via 1.0.0.2, 00:06:14, vlan2
```

According to the result, Device1 has successfully learnt the routes 2.0.0.0/24 and 200.0.0.0/24.

---

## Note

- In practical applications, if the autonomous system has 2 or more edge routers, directly redistributing routes between different routing protocols is not recommended. When configuration is necessary, routing control polices such as filtering and summarization are required on the edge routers of the autonomous system to avoid routing loops.
- 

### 60.3.3 Configure community attributes of BGP

#### Network Requirements

- EBMP neighbors are successfully established between Device1 and Device2.
- Device1 imports two direct routes 100.0.0.0/24 and 200.0.0.0/24 into BGP through the network, and sets different community attributes for the two routes when they are

advertised to Device2.

- When Device2 receives the route advertised by Device1, it filters the route 100.0.0.0/24 in the incoming direction of the neighbor by matching community attributes, and permits the route 200.0.0.0/24 to pass.

### Network Topology

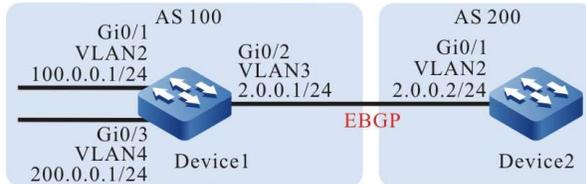


Figure 60 Network Topology for Configuring Community Attributes of BGP

### Configuration Steps

Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configure IP addresses for the ports. (Omitted)

Step 3: Configure BGP.

#### #Configure Device1.

```
Device1#configure terminal
Device1(config)#router bgp 100
Device1(config-bgp)#neighbor 2.0.0.2 remote-as 200
Device1(config-bgp)#network 100.0.0.0 255.255.255.0
Device1(config-bgp)#network 200.0.0.0 255.255.255.0
Device1(config-bgp)#exit
```

#### #Configure Device2.

```
Device2#configure terminal
Device2(config)#router bgp 200
Device2(config-bgp)#neighbor 2.0.0.1 remote-as 100
Device2(config-bgp)#exit
```

#### #View the status of BGP neighbors on Device 1.

```
Device1#show ip bgp summary
BGP router identifier 200.0.0.1, local AS number 100
BGP table version is 1
1 BGP AS-PATH entries
0 BGP community entries

Neighbor    V  AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down State/PfxRcd
2.0.0.2    4  200    2    3    1    0  0:00:00:04  0
```

#It can be seen that BGP neighbors have been successfully established between Device 1 and Device2.

#### #View the routing table on Device2.

```
Device2#show ip route bgp
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i - ISIS
U - Per-user Static route
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
B 100.0.0.0/24 [20/0] via 2.0.0.1, 00:07:47, vlan2
B 200.0.0.0/24 [20/0] via 2.0.0.1, 00:07:47, vlan2
```

According to the result, Device2 has successfully learnt the routes 100.0.0.0/24 and 200.0.0.0/24.

Step 4: Configure access list and routing policy, and set BGP community attributes.

#Configure Device1.

```
Device1(config)#ip access-list standard 1
Device1(config-std-nacl)#permit 100.0.0.0 0.0.0.255
Device1(config-std-nacl)#commit
Device1(config-std-nacl)#exit
Device1(config)#ip access-list standard 2
Device1(config-std-nacl)#permit 200.0.0.0 0.0.0.255
Device1(config-std-nacl)#commit
Device1(config-std-nacl)#exit
Device1(config)#route-map CommunitySet 10
Device1(config-route-map)#match ip address 1
Device1(config-route-map)#set community 100:1
Device1(config-route-map)#exit
Device1(config)#route-map CommunitySet 20
Device1(config-route-map)#match ip address 2
Device1(config-route-map)#set community 100:2
Device1(config-route-map)#exit
```

Set different community attributes for the routes 100.0.0.0/24 and 200.0.0.0/24 by configuring access list and routing policy.

Step 5: Configure BGP to associate with the routing policy.

#Configure Device1.

```
Device1(config)#router bgp 100
Device1(config-bgp)#neighbor 2.0.0.2 route-map CommunitySet out
Device1(config-bgp)#neighbor 2.0.0.2 send-community
Device1(config-bgp)#exit
```

#View the BGP routing table of Device2.

```
Device2#show ip bgp 100.0.0.0
BGP routing table entry for 100.0.0.0/24
Paths: (1 available, best #1, table Default-IP-Routing-Table)
Not advertised to any peer
100
 2.0.0.1 (metric 10) from 2.0.0.1 (10.0.0.1)

Origin IGP, metric 0, localpref 100, valid, external, best
Community: 100:1
Last update: 00:01:06 ago

Device2#show ip bgp 200.0.0.0
BGP routing table entry for 200.0.0.0/24
Paths: (1 available, best #1, table Default-IP-Routing-Table)
Not advertised to any peer
100
 2.0.0.1 (metric 10) from 2.0.0.1 (10.0.0.1)

Origin IGP, metric 0, localpref 100, valid, external, best
Community: 100:2
Last update: 00:01:10 ago
```

It can be seen from the BGP routing table of Device2 that the community attribute of 100.0.0.0/24 has been set as 100:1, and that of 200.0.0.0/24 as 100:2.

Step 6: Configure BGP route filtration.

#Configure Device2.

```
Device2(config)#ip community-list 1 permit 100:2
Device2(config)#route-map communityfilter
Device2(config-route-map)#match community 1
Device2(config-route-map)#exit
Device2(config)#router bgp 200
Device2(config-bgp)#neighbor 2.0.0.1 route-map communityfilter in
Device2(config-bgp)#exit
```

Step 7: Check the result.

#View the routing table of Device 2.

```
Device2#show ip route bgp
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
U - Per-user Static route
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

B 200.0.0.0/24 [20/0] via 2.0.0.1, 00:00:53, vlan2
```

It can be seen from the BGP routing table of Device2 that 100.0.0.0/24 is filtered in the incoming direction, while 200.0.0.0/24 is allowed to pass.

---

### Note

- After configuring routing policy on the peer, it is required to reset the BGP process to make it take effect.
  - The command send-community is required to advertise the community attributes to the peer.
- 

## 60.3.4 Configure BGP Route Reflector

### Network Requirements

- Device3 establishes EBGP neighbors with Device4 which advertises the route of the 100.0.0.0/24 to Device3.
- Device2 establishes IBGP neighbors with Device3 and Device1 respectively. Route reflector is configured on Device2. Device1 and Device3 serve as clients so that Device1 can learn the route 100.0.0.0/24 advertised by Device4.

### Network Topology

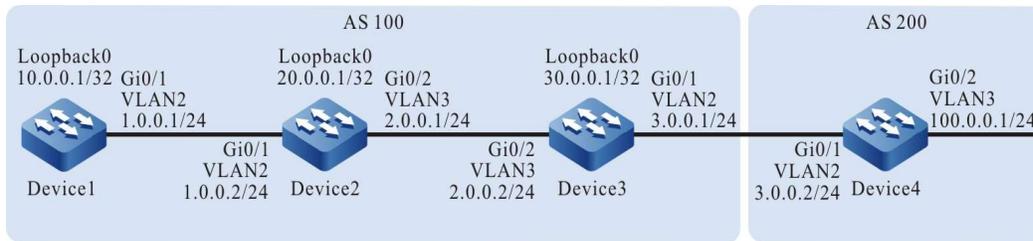


Figure 60 Network Topology for Configuring BGP Route Reflector

### Configuration Steps

- Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)
- Step 2: Configure IP addresses for the ports. (Omitted)
- Step 3: Configure OSPF so that the routes of Loopback between devices are reachable from each other.

#### #Configure Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#network 1.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 10.0.0.1 0.0.0.0 area 0
Device1(config-ospf)#exit
```

#### #Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 1.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#network 20.0.0.1 0.0.0.0 area 0
Device2(config-ospf)#exit
```

#### #Configure Device3.

```
Device2#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 30.0.0.1 0.0.0.0 area 0
Device3(config-ospf)#exit
```

#### #View the routing table of Device1.

```
Device1#show ip route ospf
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
U - Per-user Static route
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

O 2.0.0.0/24 [110/2] via 1.0.0.2, 01:12:00, vlan2
O 20.0.0.1/32 [110/2] via 1.0.0.2, 01:11:47, vlan2
O 30.0.0.1/32 [110/3] via 1.0.0.2, 01:07:47, vlan2
```

#### #View the routing table of Device 2.

```
Device2#show ip route ospf
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
U - Per-user Static route
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

- 10.0.0.1/32 [110/2] via 1.0.0.1, 01:13:02, vlan2
- 30.0.0.1/32 [110/2] via 2.0.0.2, 01:08:58, vlan3

#### #Check the routing table of Device3.

```
Device3#show ip route ospf
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

O 1.0.0.0/24 [110/2] via 2.0.0.1, 01:10:04, vlan2
O 10.0.0.1/32 [110/3] via 2.0.0.1, 01:10:04, vlan2
O 20.0.0.1/32 [110/2] via 2.0.0.1, 01:10:04, vlan2
```

It can be seen that Device1, Device2 and Device3 can learn the routes of their loopback interface from each other.

#### Step 4: Configure BGP.

##### #Configure Device1.

```
Device1(config)#router bgp 100
Device1(config-bgp)#neighbor 20.0.0.1 remote-as 100
Device1(config-bgp)#neighbor 20.0.0.1 update-source loopback0
Device1(config-bgp)#exit
```

##### #Configure Device2.

```
Device2(config)#router bgp 100
Device2(config-bgp)#neighbor 30.0.0.1 remote-as 100
Device2(config-bgp)#neighbor 30.0.0.1 update-source loopback0
Device2(config-bgp)#neighbor 10.0.0.1 remote-as 100
Device2(config-bgp)#neighbor 10.0.0.1 update-source loopback0
Device2(config-bgp)#exit
```

##### #Configure Device3.

```
Device3(config)#router bgp 100
Device3(config-bgp)#neighbor 3.0.0.2 remote-as 200
Device3(config-bgp)#neighbor 20.0.0.1 remote-as 100
Device3(config-bgp)#neighbor 20.0.0.1 update-source loopback0
Device3(config-bgp)#neighbor 20.0.0.1 next-hop-self
Device3(config-bgp)#exit
```

##### #Configure Device4.

```
Device4#configure terminal
Device4(config)#router bgp 200
Device4(config-bgp)#neighbor 3.0.0.1 remote-as 100
Device4(config-bgp)#network 100.0.0.0 255.255.255.0
Device4(config-bgp)#exit
```

##### #View the status of BGP neighbors on Device 2.

```
Device2#show ip bgp summary
BGP router identifier 20.0.0.1, local AS number 100
BGP table version is 1
2 BGP AS-PATH entries
0 BGP community entries

Neighbor    V  AS MsgRcvd MsgSent  TblVer  InQ  OutQ  Up/Down  State/PfxRcd
10.0.0.1    4 100    8     8     1  0  0 00:03:01    0
30.0.0.1    4 100    9     9     1  0  0 00:02:41    1
```

##### #View the status of BGP neighbors on Device4.

```

Device4#show ip bgp summary
BGP router identifier 100.0.0.1, local AS number 200
BGP table version is 1
1 BGP AS-PATH entries
0 BGP community entries

Neighbor      V  AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down State/PfxRcd
3.0.0.1      4 100   19    19      1    0  00:05:40    0

```

It can be seen that BGP neighbors have been successfully established between devices.

#View the BGP routing table of Device3.

```

Device3#show ip bgp
BGP table version is 2, local router ID is 30.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Network      Next Hop      Metric LocPrf Weight Path
[B]*> 100.0.0.0/24  3.0.0.2        0      0 200 i

```

#View the BGP routing table of Device2.

```

Device2#show ip bgp
BGP table version is 768, local router ID is 20.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Network      Next Hop      Metric LocPrf Weight Path
[B]*>i100.0.0.0/24  30.0.0.1      0    100  0 200 i

```

#View the BGP routing table on Device1.

```

Device1#show ip bgp
BGP table version is 2, local router ID is 10.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Network      Next Hop      Metric LocPrf Weight Path

```

It can be seen from above that both Device2 and Device3 have learned the route 100.0.0.0/24, though Device2 doesn't advertise it to Device1.

Step 5: Configure BGP route reflector.

#Configure Device2.

```

Device2(config)#router bgp 100
Device2(config-bgp)#neighbor 10.0.0.1 route-reflector-client
Device2(config-bgp)#neighbor 30.0.0.1 route-reflector-client
Device2(config-bgp)#exit

```

On Device2, configure Device1 and Device3 as clients of route reflector.

Step 6: Check the result.

#View the routing table of Device1.

```

Device1#show ip bgp
BGP table version is 2, local router ID is 10.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

```

```

Network      Next Hop      Metric LocPrf Weight Path
[B]*>i100.0.0.0/24 30.0.0.1      0 100 0 200 i

```

```

Device1#show ip route bgp
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
U - Per-user Static route
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

```

```

B 100.0.0.0/24 [200/0] via 30.0.0.1, 00:01:40, vlan2

```

Configure Device1 and Device3 as clients of route reflector in the BGP of Device2 which successfully reflects the route 100.0.0.0/24 to the client Device1.

## Note

- When a peer is configured as the client of route reflector, the neighbors of the device and this peer will be reset.

### 60.3.5 Configure BGP route aggregation

#### Network Requirements

- Device1 establishes OSPF neighbors with Device3 which advertises the two routes 100.1.0.0/24 and 100.2.0.0/24 to Device1.
- EBMP neighbors are successfully established between Device1 and Device2.
- On Device1, the routes 100.1.0.0/24 and 100.2.0.0/24 are aggregated into 100.0.0.0/14 to advertise to Device2.

#### Network Topology

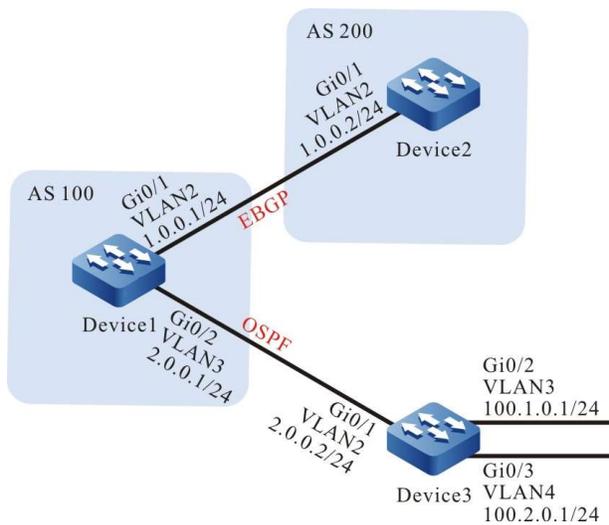


Figure 60 Network Topology for Configuring BGP Route Aggregation

## Configuration Steps

Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configure IP addresses for the ports. (Omitted)

Step 3: Configure OSPF so that the routes of Loopback between devices are reachable from each other.

### #Configure Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#exit
```

### #Configure Device3.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 100.1.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 100.2.0.0 0.0.0.255 area 0
Device3(config-ospf)#exit
```

### #View the routing table of Device1.

```
Device1#show ip route ospf
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

O 100.1.0.0/24 [110/2] via 2.0.0.2, 00:00:24, vlan3
O 100.2.0.0/24 [110/2] via 2.0.0.2, 00:00:24, vlan3
```

According to the result, Device1 learns the two routes 100.1.0.0/24 and 100.2.0.0/24 distributed by Device3.

Step 4: Configure BGP.

### #Configure Device1.

```
Device1(config)#router bgp 100
Device1(config-bgp)#neighbor 1.0.0.2 remote-as 200
Device1(config-bgp)#exit
```

### #Configure Device2.

```
Device2#configure terminal
Device2(config)#router bgp 200
Device2(config-bgp)#neighbor 1.0.0.1 remote-as 100
Device2(config-bgp)#exit
```

### #View the status of BGP neighbors on Device 1.

```
Device1#show ip bgp summary
BGP router identifier 1.0.0.1, local AS number 100
BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries

Neighbor    V  AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down State/PfxRcd
```

```
1.0.0.2 4 200 2 2 2 0 0 00:00:42 0
```

BGP neighbor has been successfully established between Device1 and Device2.

Step 5: Configure BGP route aggregation.

To meet the network requirements, here are two schemes:

Scheme 1: Configure the aggregated static route pointing to null0 and import it into BGP.

#Configure Device1.

```
Device1(config)#ip route 100.0.0.0 255.252.0.0 null0
Device1(config)#router bgp 100
Device1(config-bgp)#network 100.0.0.0 255.252.0.0
Device1(config-bgp)#exit
```

Check the result.

#View the BGP routing table on Device1.

```
Device1#show ip bgp
BGP table version is 2, local router ID is 10.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
              Network      Next Hop      Metric LocPrf Weight Path
[B]*> 100.0.0.0/14      0.0.0.0          32768 i
```

It can be seen that the aggregated route 100.0.0.0/14 has been generated in the BGP routing table of Device1.

#View the routing table of Device 2.

```
Device2#show ip bgp
BGP table version is 3, local router ID is 20.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
              Network      Next Hop      Metric LocPrf Weight Path
[B]*> 100.0.0.0/14      1.0.0.1          0      0 100 i

Device2#show ip route bgp
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

B 100.0.0.0/14 [20/0] via 1.0.0.1, 01:39:30, vlan2
```

It can be seen that Device2 has successfully learned the aggregated route 100.0.0.0/14 advertised by Device1.

Scheme 2: First import the detail route into BGP and then complete route aggregation via the command **aggregate-address**.

#Configure Device1.

```
Device1(config)#router bgp 100
Device1(config-bgp)#redistribute ospf 100
Device1(config-bgp)#aggregate-address 100.0.0.0 255.252.0.0 summary-only
Device1(config-bgp)#exit
```

Check the result.

#View the BGP routing table on Device1.

```
Device1#show ip bgp
BGP table version is 2, local router ID is 10.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop        Metric LocPrf Weight Path
[B]*> 100.0.0.0/14  0.0.0.0          32768 i
[B]s> 100.1.0.0/24  2.0.0.2           2   32768 i
[B]s> 100.2.0.0/24  2.0.0.2           2   32768 i
```

It can be seen that the aggregated route 100.0.0.0/14 has been generated in the BGP routing table of Device1.

#View the routing table of Device 2.

```
Device2#show ip bgp
BGP table version is 3, local router ID is 20.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop        Metric LocPrf Weight Path
[B]*> 100.0.0.0/14  1.0.0.1           0     0 100 i

Device2#show ip route bgp
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

B 100.0.0.0/14 [20/0] via 1.0.0.1, 01:39:30, vlan2
```

It can be seen that Device2 has successfully learned the aggregated route 100.0.0.0/14 advertised by Device1.

---

## Note

- When the command `aggregate-address` is used for route aggregation, if the extension command `summary-only` is configured, the device will advertise aggregated route only; otherwise, it will advertise both detail route and aggregated route.
- 

## 60.3.6 Configure BGP route preference

### Network Requirements

- Device1 has established IBGP neighbors with Device2 and Device3, and Device4 has established EBGP neighbors with Device2 and Device3.
- Device1 advertises two routes to Device4, i.e. 55.0.0.0/24 and 65.0.0.0/24; Device4 advertises two routes to Device1, i.e. 75.0.0.0/24 and 85.0.0.0/24.
- By modifying the Local-preference of route on Device2 and Device3, you can make

Device1 prefer the route 75.0.0.0/24 advertised by Device2 and the route 85.0.0.0/24 advertised by Device3.

- By modifying the MED of route on Device2 and Device3, you can make Device4 prefer the route 55.0.0.0/24 advertised by Device2 and the route 65.0.0.0/24 advertised by Device3.

## Network Topology

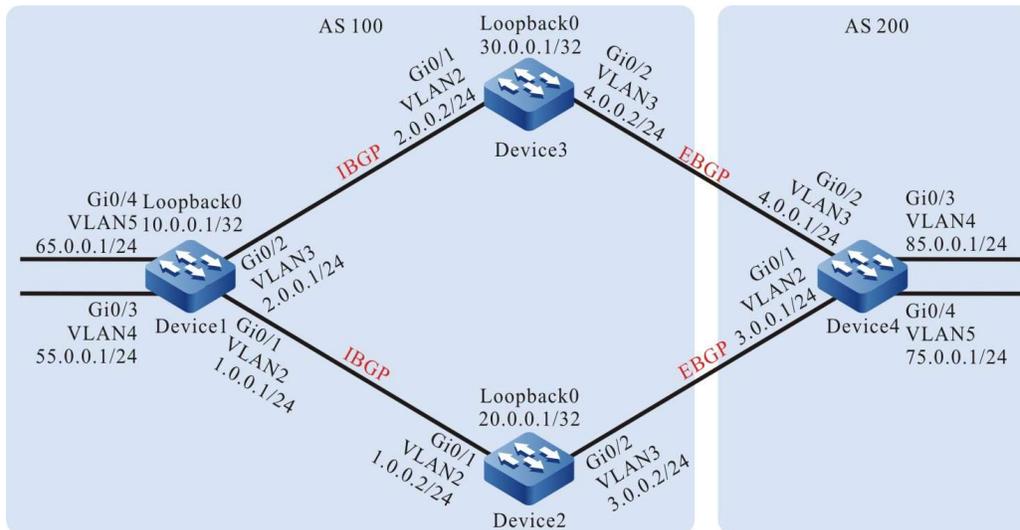


Figure 60 Network Topology for Configuring BGP Route Preference

## Configuration Steps

- Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)
- Step 2: Configure IP addresses for the ports. (Omitted)
- Step 3: Configure OSPF so that the routes of Loopback between devices are reachable from each other.

### #Configure Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#network 1.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 10.0.0.1 0.0.0.0 area 0
Device1(config-ospf)#exit
```

### #Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 1.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#network 20.0.0.1 0.0.0.0 area 0
Device2(config-ospf)#exit
```

### #Configure Device3.

```
Device3#configure terminal
```

```
Device3(config)#router ospf 100
Device3(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 30.0.0.1 0.0.0.0 area 0
Device3(config-ospf)#exit
```

#### #View the routing table of Device1.

```
Device1#show ip route ospf
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

O 20.0.0.1/32 [110/2] via 1.0.0.2, 00:03:15, vlan2
O 30.0.0.1/32 [110/2] via 2.0.0.2, 00:01:40, vlan3
```

#### #View the routing table of Device 2.

```
Device2#show ip route ospf
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

O 2.0.0.0/24 [110/2] via 1.0.0.1, 00:03:54, vlan2
O 10.0.0.1/32 [110/2] via 1.0.0.1, 00:03:54, vlan2
O 30.0.0.1/32 [110/3] via 1.0.0.1, 00:02:14, vlan2
```

#### #Check the routing table of Device3.

```
Device3#show ip route ospf
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

O 1.0.0.0/24 [110/2] via 2.0.0.1, 00:02:35, vlan2
O 10.0.0.1/32 [110/2] via 2.0.0.1, 00:02:35, vlan2
O 20.0.0.1/32 [110/3] via 2.0.0.1, 00:02:35, vlan2
```

It can be seen that Device1, Device2 and Device3 can learn the routes of their loopback interface from each other.

#### Step 4: Configure BGP.

##### #Configure Device1.

```
Device1(config)#router bgp 100
Device1(config-bgp)#neighbor 20.0.0.1 remote-as 100
Device1(config-bgp)#neighbor 20.0.0.1 update-source loopback0
Device1(config-bgp)#neighbor 30.0.0.1 remote-as 100
Device1(config-bgp)#neighbor 30.0.0.1 update-source loopback0
Device1(config-bgp)#network 55.0.0.0 255.255.255.0
Device1(config-bgp)#network 65.0.0.0 255.255.255.0
Device1(config-bgp)#exit
```

##### #Configure Device2.

```
Device2(config)#router bgp 100
Device2(config-bgp)#neighbor 10.0.0.1 remote-as 100
Device2(config-bgp)#neighbor 10.0.0.1 update-source loopback0
Device2(config-bgp)#neighbor 10.0.0.1 next-hop-self
Device2(config-bgp)#neighbor 3.0.0.1 remote-as 200
Device2(config-bgp)#exit
```

##### #Configure Device3.

```
Device3(config)#router bgp 100
Device3(config-bgp)#neighbor 10.0.0.1 remote-as 100
Device3(config-bgp)#neighbor 10.0.0.1 update-source loopback0
```

```
Device3(config-bgp)#neighbor 10.0.0.1 next-hop-self
Device3(config-bgp)#neighbor 4.0.0.1 remote-as 200
Device3(config-bgp)#exit
```

#### #Configure Device4.

```
Device4#configure terminal
Device4(config)#router bgp 200
Device4(config-bgp)#neighbor 3.0.0.2 remote-as 100
Device4(config-bgp)#neighbor 4.0.0.2 remote-as 100
Device4(config-bgp)#network 75.0.0.0 255.255.255.0
Device4(config-bgp)#network 85.0.0.0 255.255.255.0
Device4(config-bgp)#exit
```

#### #View the status of BGP neighbors on Device 1.

```
Device1#show ip bgp summary
BGP router identifier 10.0.0.1, local AS number 100
BGP table version is 2
2 BGP AS-PATH entries
0 BGP community entries

Neighbor    V  AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State/PfxRcd
20.0.0.1    4 100   11    11     2    0 00:07:40    2
30.0.0.1    4 100    7     7     2    0 00:03:59    2
```

#### #View the status of BGP neighbors on Device4.

```
Device4#show ip bgp summary
BGP router identifier 85.0.0.1, local AS number 200
BGP table version is 2
2 BGP AS-PATH entries
0 BGP community entries

Neighbor    V  AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State/PfxRcd
3.0.0.2     4 100    5     6     2    0 00:02:24    2
4.0.0.2     4 100    6     5     2    0 00:02:24    2
```

According to the result, Device1 has successfully established IBGP neighbors with Device2 and Device3, and Device4 has successfully established EBGP neighbors with Device2 and Device3.

#### #View the routing table of Device1.

```
Device1#show ip bgp
BGP table version is 2, local router ID is 10.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop        Metric LocPrf Weight Path
[B]*> 55.0.0.0/24  0.0.0.0          0   32768 i
[B]*> 65.0.0.0/24  0.0.0.0          0   32768 i
[B]* i75.0.0.0/24  30.0.0.1         0 100  0 200 i
[B]*>i            20.0.0.1         0 100  0 200 i
[B]* i85.0.0.0/24  30.0.0.1         0 100  0 200 i
[B]*>i            20.0.0.1         0 100  0 200 i

Device1#show ip route bgp
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

B 75.0.0.0/24 [200/0] via 20.0.0.1, 01:13:17, vlan2
B 85.0.0.0/24 [200/0] via 20.0.0.1, 01:13:17, vlan2
```

It can be seen that both 75.0.0.0/24 and 85.0.0.0/24 on Device1 select Device2 as the optimal next hop device.

#### #View the routing table of Device 4.

```

Device4#show ip bgp
BGP table version is 2, local router ID is 85.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop        Metric LocPrf Weight Path
[B]* 55.0.0.0/24   3.0.0.2         0      0 100 i
[B]*> 55.0.0.0/24 4.0.0.2         0      0 100 i
[B]* 65.0.0.0/24   3.0.0.2         0      0 100 i
[B]*> 65.0.0.0/24 4.0.0.2         0      0 100 i
[B]*> 75.0.0.0/24 0.0.0.0         0     32768 i
[B]*> 85.0.0.0/24 0.0.0.0         0     32768 i

Device4#show ip route bgp
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

B 55.0.0.0/24 [20/0] via 4.0.0.2, 01:25:19, vlan3
B 65.0.0.0/24 [20/0] via 4.0.0.2, 01:25:19, vlan3

```

It can be seen that both 55.0.0.0/24 and 65.0.0.0/24 on Device4 select Device3 as the optimal next hop device.

Step 5: Configure access control list and routing policy, and set local-preference and metric.

#Configure Device2.

```

Device2(config)#ip access-list standard 1
Device2(config-std-nacl)#permit 75.0.0.0 0.0.0.255
Device2(config-std-nacl)#commit
Device2(config-std-nacl)#exit
Device2(config)#ip access-list standard 2
Device2(config-std-nacl)#permit 65.0.0.0 0.0.0.255
Device2(config-std-nacl)#commit
Device2(config-std-nacl)#exit
Device2(config)#route-map SetPriority1 10
Device2(config-route-map)#match ip address 1
Device2(config-route-map)#set local-preference 110
Device2(config-route-map)#exit
Device2(config)#route-map SetPriority1 20
Device2(config-route-map)#exit
Device2(config)#route-map SetPriority2 10
Device2(config-route-map)#match ip address 2
Device2(config-route-map)#set metric 100
Device2(config-route-map)#exit
Device2(config)#route-map SetPriority2 20
Device2(config-route-map)#exit

```

Configure routing policy on Device2 to set the local-preference of 75.0.0.0/24 as 110 and the metric of 65.0.0.0/24 as 100.

#Configure Device3.

```

Device3(config)#ip access-list standard 1
Device3(config-std-nacl)#permit 85.0.0.0 0.0.0.255
Device3(config-std-nacl)#commit
Device3(config-std-nacl)#exit
Device3(config)#ip access-list standard 2
Device3(config-std-nacl)#permit 55.0.0.0 0.0.0.255
Device3(config-std-nacl)#commit
Device3(config-std-nacl)#exit
Device3(config)#route-map SetPriority1 10
Device3(config-route-map)#match ip address 1
Device3(config-route-map)#set local-preference 110
Device3(config-route-map)#exit
Device3(config)#route-map SetPriority1 20

```

```

Device3(config-route-map)#exit
Device3(config)#route-map SetPriority2 10
Device3(config-route-map)#match ip address 2
Device3(config-route-map)#set metric 100
Device3(config-route-map)#exit
Device3(config)#route-map SetPriority2 20
Device3(config-route-map)#exit

```

Configure routing policy on Device3 to set the local-preference of 85.0.0.0/24 as 110 and the metric of 55.0.0.0/24 as 100.

---

## Note

- When configuring a routing policy, both the prefix list and ACL can create filtering rules. The difference is that the prefix list can exactly match the routing mask.
- 

Step 6: Configure BGP to associate with the routing policy.

#Configure Device2.

```

Device2(config)#router bgp 100
Device2(config-bgp)#neighbor 10.0.0.1 route-map SetPriority1 out
Device2(config-bgp)#neighbor 3.0.0.1 route-map SetPriority2 out
Device2(config-bgp)#exit

```

On Device2, modify the local-preference of 75.0.0.0/24 in the outgoing direction of neighbor 10.0.0.1 and the metric of 65.0.0.0/24 in the outgoing direction of neighbor 3.0.0.1.

#Configure Device3.

```

Device3(config)#router bgp 100
Device3(config-bgp)#neighbor 10.0.0.1 route-map SetPriority1 out
Device3(config-bgp)#neighbor 4.0.0.1 route-map SetPriority2 out
Device3(config-bgp)#exit

```

On Device3, modify the local-preference of 85.0.0.0/24 in the outgoing direction of neighbor 10.0.0.1 and the metric of 55.0.0.0/24 in the outgoing direction of neighbor 4.0.0.1.

After configuring routing policy on the peer, it is required to reset the BGP process to make it take effect.

Step 7: Check the result.

#View the routing table of Device1.

```

Device1#show ip bgp
BGP table version is 5, local router ID is 10.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

```

Network	Next Hop	Metric	LocPrf	Weight	Path
[B]*> 55.0.0.0/24	0.0.0.0	0			32768 i
[B]*> 65.0.0.0/24	0.0.0.0	0			32768 i
[B]* i75.0.0.0/24	30.0.0.1	0	100	0	200 i
[B]*>i	20.0.0.1	0	110	0	200 i
[B]*>i85.0.0.0/24	30.0.0.1	0	110	0	200 i

```
[B]* i      20.0.0.1      0 100  0 200 i
```

```
Device1#show ip route bgp
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
U - Per-user Static route
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
B 75.0.0.0/24 [200/0] via 20.0.0.1, 00:01:34, vlan2
B 85.0.0.0/24 [200/0] via 30.0.0.1, 00:00:51, vlan3
```

It can be seen that the local-preference values of 75.0.0.0/24 and 85.0.0.0/24 have been successfully modified, and Device1 prefers the route 75.0.0.0/24 advertised by Device2 and the route 85.0.0.0/24 advertised by Device3.

#View the routing table of Device 4.

```
Device4#show ip bgp
BGP table version is 4, local router ID is 85.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Network        Next Hop      Metric LocPrf Weight Path
[B]* 55.0.0.0/24  4.0.0.2      100    0 100 i
[B]*>          3.0.0.2      0      0 100 i
[B]*> 65.0.0.0/24  4.0.0.2      0      0 100 i
[B]*          3.0.0.2      100    0 100 i
[B]*> 75.0.0.0/24  0.0.0.0      0     32768 i
[B]*> 85.0.0.0/24  0.0.0.0      0     32768 i
```

```
Device4#show ip route bgp
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
U - Per-user Static route
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
B 55.0.0.0/24 [20/0] via 3.0.0.2, 00:15:02, vlan2
B 65.0.0.0/24 [20/0] via 4.0.0.2, 00:14:55, vlan3
```

It can be seen that the metric values of 55.0.0.0/24 and 65.0.0.0/24 have been successfully modified, and Device4 prefers the route 55.0.0.0/24 advertised by Device2 and the route 65.0.0.0/24 advertised by Device3.

---

## Note

- Routing policy can be used either in the outgoing direction of route advertisement or in the incoming direction of route receiving.
- 

## 60.3.7 Configure BGP Confederation

### Network Requirements

- Device2, Device3, Device4 and Device5 are within the same BGP AS 200. In order to reduce IBGP full connections, you can incorporate them into two different AS within the same BGP confederation.

- Device1 establishes EBGP neighbors with Device2 and advertises the route 100.0.0.0/24 to AS 200.

### Network Topology

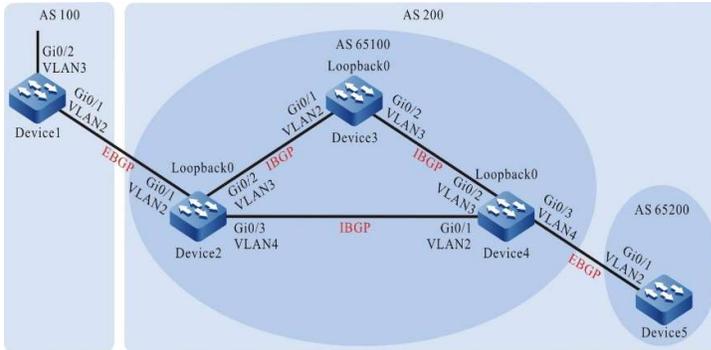


Figure 60 Network Topology for Configuring BGP Confederation

of equipment	Interface	VLAN	IP address
Device1	Gi0/1	2	1.0.0.1/24
	Gi0/2	3	100.0.0.1/24
Device2	Gi0/1	2	1.0.0.2/24
	Gi0/2	3	2.0.0.2/24
	Gi0/3	4	3.0.0.2/24
	Loopback0		20.0.0.1/32
Device3	Gi0/1	2	2.0.0.1/24
	Gi0/2	3	4.0.0.1/24
	Loopback0		30.0.0.1/32
Device4	Gi0/1	2	3.0.0.1/24
	Gi0/2	3	4.0.0.2/24
	Gi0/3	4	5.0.0.1/24
	Loopback0		40.0.0.1/32

of equipment	Interface	VLAN	IP address
Device5	Gi0/1	2	5.0.0.2/24

### Configuration Steps

Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configure IP addresses for the ports. (Omitted)

Step 3: Configure OSPF so that the routes of Loopback between devices are reachable from each other.

#### #Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#network 3.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#network 20.0.0.1 0.0.0.0 area 0
Device2(config-ospf)#exit
```

#### #Configure Device3.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 4.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 30.0.0.1 0.0.0.0 area 0
Device3(config-ospf)#exit
```

#### #Configure Device4.

```
Device4#configure terminal
Device4(config)#router ospf 100
Device4(config-ospf)#network 3.0.0.0 0.0.0.255 area 0
Device4(config-ospf)#network 4.0.0.0 0.0.0.255 area 0
Device4(config-ospf)#network 5.0.0.0 0.0.0.255 area 0
Device4(config-ospf)#network 40.0.0.1 0.0.0.0 area 0
Device4(config-ospf)#exit
```

#### #Configure Device5.

```
Device5#configure terminal
Device5(config)#router ospf 100
Device5(config-ospf)#network 5.0.0.0 0.0.0.255 area 0
Device5(config-ospf)#exit
```

#### #View the routing table of Device 2.

```
Device2#show ip route ospf
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

O 4.0.0.0/24 [110/2] via 2.0.0.1, 00:02:42, vlan3
   [110/2] via 3.0.0.1, 00:02:11, vlan4
O 30.0.0.1/32 [110/2] via 2.0.0.1, 00:02:32, vlan3
O 40.0.0.1/32 [110/2] via 3.0.0.1, 00:02:05, vlan4
```

### #Check the routing table of Device3.

```
Device3#show ip route ospf
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
U - Per-user Static route
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

O 3.0.0.0/24 [110/2] via 2.0.0.2, 00:03:24, vlan2
   [110/2] via 4.0.0.2, 00:02:38, vlan3
O 20.0.0.1/32 [110/2] via 2.0.0.2, 00:03:24, vlan2
O 40.0.0.1/32 [110/2] via 4.0.0.2, 00:02:38, vlan3
```

### #View the routing table of Device 4.

```
Device4#show ip route ospf
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
U - Per-user Static route
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

O 2.0.0.0/24 [110/2] via 3.0.0.2, 00:03:42, vlan2
   [110/2] via 4.0.0.1, 00:03:42, vlan3
O 20.0.0.1/32 [110/2] via 3.0.0.2, 00:03:42, vlan2
O 30.0.0.1/32 [110/2] via 4.0.0.1, 00:03:42, vlan3
```

### #View the routing table of Device5.

```
Device5#show ip route ospf
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
U - Per-user Static route
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

O 2.0.0.0/24 [110/3] via 5.0.0.1, 00:00:03, vlan2
O 3.0.0.0/24 [110/2] via 5.0.0.1, 00:00:03, vlan2
O 4.0.0.0/24 [110/2] via 5.0.0.1, 00:00:03, vlan2
O 20.0.0.1/32 [110/3] via 5.0.0.1, 00:00:03, vlan2
O 30.0.0.1/32 [110/3] via 5.0.0.1, 00:00:03, vlan2
O 40.0.0.1/32 [110/2] via 5.0.0.1, 00:00:03, vlan2
```

It can be seen that Device2, Device3 and Device4 can learn the routes of their loopback interface from each other.

Step 4: Configure BGP connections within the confederation.

### #Configure IBGP connections within the confederation.

#### #Configure Device2.

```
Device2(config)#router bgp 65100
Device2(config-bgp)#neighbor 30.0.0.1 remote-as 65100
Device2(config-bgp)#neighbor 30.0.0.1 update-source loopback0
Device2(config-bgp)#neighbor 40.0.0.1 remote-as 65100
Device2(config-bgp)#neighbor 40.0.0.1 update-source loopback0
Device2(config-bgp)#neighbor 30.0.0.1 next-hop-self
Device2(config-bgp)#neighbor 40.0.0.1 next-hop-self
Device2(config-bgp)#exit
```

#### #Configure Device3.

```
Device3(config)#router bgp 65100
Device3(config-bgp)#neighbor 20.0.0.1 remote-as 65100
Device3(config-bgp)#neighbor 20.0.0.1 update-source loopback0
Device3(config-bgp)#neighbor 40.0.0.1 remote-as 65100
Device3(config-bgp)#neighbor 40.0.0.1 update-source loopback0
Device3(config-bgp)#exit
```

#### #Configure Device4.

```

Device4(config)#router bgp 65100
Device4(config-bgp)#neighbor 20.0.0.1 remote-as 65100
Device4(config-bgp)#neighbor 20.0.0.1 update-source loopback0
Device4(config-bgp)#neighbor 30.0.0.1 remote-as 65100
Device4(config-bgp)#neighbor 30.0.0.1 update-source loopback0
Device4(config-bgp)#exit

```

#Configure EBGP connections within the confederation

#Configure Device4.

```

Device4(config)#router bgp 65100
Device4(config-bgp)#neighbor 5.0.0.2 remote-as 65200
Device4(config-bgp)#exit

```

#Configure Device5.

```

Device5(config)#router bgp 65200
Device5(config-bgp)#neighbor 5.0.0.1 remote-as 65100
Device5(config-bgp)#exit

```

#View the status of BGP neighbors on Device4.

```

Device4#show ip bgp summary
BGP router identifier 40.0.0.1, local AS number 65100
BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries

Neighbor    V  AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down State/PfxRcd
5.0.0.2     4 65200  15   15    2  0  0 00:09:40  0
20.0.0.1    4 65100   9    9    2  0  0 00:07:49  0
30.0.0.1    4 65100   7    7    2  0  0 00:05:39  0

```

Device4 has established IBGP neighbors with Device2 and Device3, and Device4 has established EBGP neighbors with Device5.

Step 5: Configure BGP confederation.

#Configure Device1.

Configure EBGP peer. The peer AS number is the confederation ID 200.

```

Device1#configure terminal
Device1(config)#router bgp 100
Device1(config-bgp)#neighbor 1.0.0.2 remote-as 200
Device1(config-bgp)#network 100.0.0.0 255.255.255.0
Device1(config-bgp)#exit

```

#Configure Device2.

Configure the BGP confederation ID as 200 and EBGP peer (AS number 100).

```

Device2(config)#router bgp 65100
Device2(config-bgp)#bgp confederation identifier 200
Device2(config-bgp)#neighbor 1.0.0.1 remote-as 100
Device2(config-bgp)#exit

```

#Configure Device3.

Configure the BGP confederation ID as 200.

```

Device3(config)#router bgp 65100
Device3(config-bgp)#bgp confederation identifier 200
Device3(config-bgp)#exit

```

#Configure Device4.

Configure the BGP confederation ID as 200, and make the confederation contain area 65100.

```
Device4#configure terminal
Device4(config)#router bgp 65100
Device4(config-bgp)#bgp confederation identifier 200
Device4(config-bgp)#bgp confederation peers 65200
Device4(config-bgp)#exit
```

#Configure Device5.

Configure the BGP confederation ID as 200, and make the confederation contain area 65200.

```
Device5(config)#router bgp 65200
Device5(config-bgp)#bgp confederation identifier 200
Device5(config-bgp)#bgp confederation peers 65100
Device5(config-bgp)#exit
```

Step 6: Check the result.

#View the status of BGP neighbors on Device 1.

```
Device1#show ip bgp summary
BGP router identifier 100.0.0.1, local AS number 100
BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries

Neighbor    V  AS MsgRcvd MsgSent  TblVer  InQ  OutQ  Up/Down  State/PfxRcd
1.0.0.2    4 200    6    6    2  0  00:02:20  0
```

#It can be seen that EBGP neighbor relation has been successfully established between Device 1 and Device2.

#View the routing information on Device5.

```
Device5#show ip bgp
BGP table version is 49, local router ID is 5.0.0.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Network      Next Hop        Metric LocPrf Weight Path
[B]*> 100.0.0.0/24  20.0.0.1          0  100  0 (65100) 100 i

Device5#show ip route bgp
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

B 100.0.0.0/24 [200/0] via 20.0.0.1, 00:00:38, vlan2
```

Device5 has successfully learned the route 100.0.0.0/24, and it can be seen that the next-hop attribute keeps unchanged when this route is transmitted in the confederation. Device2, Device3, Device4 and Device5 all belong to the same confederation. So full connections are not required. Device5 obtains external routing information through Device4.

## 60.3.8 Configure BGP to Coordinate with BFD

### Network Requirements

- Device1 establishes EBGP neighbors with Device2 and Device3, and IBGP neighbors are

established between Device2 and Device3.

- Device1 learns theEBGP route 3.0.0.0/24 from Device2 and Device3 at the same time, and prefers Device2 to forward data to the network segment 3.0.0.0/24.
- Configure EBGP to associate BFD on Device1 and Device2. When the line between Device1 and Device2 fails, BFD can quickly detect and notify BGP. Then, Device1 chooses Device3 to forward data to the network segment 3.0.0.0/24.

### Network Topology

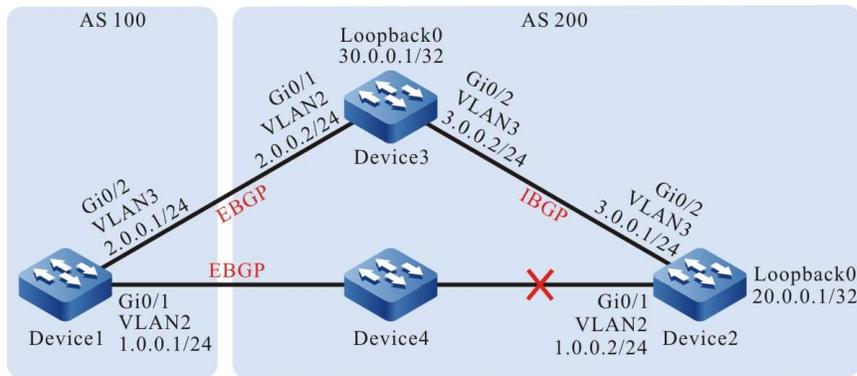


Figure 60 Network Topology for Configuring Coordination of BGP with BFD

### Configuration Steps

- Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)
- Step 2: Configure IP addresses for the ports. (Omitted)
- Step 3: Configure OSPF so that the routes of Loopback between devices are reachable from each other.

#### #Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 3.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#network 20.0.0.1 0.0.0.0 area 0
Device2(config-ospf)#exit
```

#### #Configure Device3.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#network 3.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 30.0.0.1 0.0.0.0 area 0
Device3(config-ospf)#exit
```

#### #View the routing table of Device 2.

```
Device2#show ip route ospf
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
U - Per-user Static route
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
O 30.0.0.1/32 [110/2] via 3.0.0.2, 00:02:26, vlan3
```

#Check the routing table of Device3.

```
Device3#show ip route ospf
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

O 20.0.0.1/32 [110/2] via 3.0.0.1, 00:03:38, vlan3
```

It can be seen that Device2 and Device3 can learn the routes of their loopback interface from each other.

Step 4: Configure access control list and routing policy, and set the routing metric.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#ip access-list standard 1
Device1(config-std-nacl)#permit 3.0.0.0 0.0.0.255
Device1(config-std-nacl)#commit
Device1(config-std-nacl)#exit
Device1(config)#route-map SetMetric
Device1(config-route-map)#match ip address 1
Device1(config-route-map)#set metric 50
Device1(config-route-map)#exit
```

On Device1, configure the routing policy and set the metric value of 3.0.0.0/24 as 50.

Step 5: Configure BGP and associate routing policy on Device1.

#Configure Device1.

```
Device1(config)#router bgp 100
Device1(config-bgp)#neighbor 1.0.0.2 remote-as 200
Device1(config-bgp)#neighbor 2.0.0.2 remote-as 200
Device1(config-bgp)#neighbor 2.0.0.2 route-map SetMetric in
Device1(config-bgp)#exit
```

#Configure Device2.

```
Device2(config)#router bgp 200
Device2(config-bgp)#neighbor 1.0.0.1 remote-as 100
Device2(config-bgp)#neighbor 30.0.0.1 remote-as 200
Device2(config-bgp)#neighbor 30.0.0.1 update-source loopback0
Device2(config-bgp)#network 3.0.0.0 255.255.255.0
Device2(config-bgp)#exit
```

#Configure Device3.

```
Device3(config)#router bgp 200
Device3(config-bgp)#neighbor 2.0.0.1 remote-as 100
Device3(config-bgp)#neighbor 20.0.0.1 remote-as 200
Device3(config-bgp)#neighbor 20.0.0.1 update-source loopback0
Device3(config-bgp)#network 3.0.0.0 255.255.255.0
Device3(config-bgp)#exit
```

After configuring routing policy on the peer, it is required to reset the BGP process to make it take effect.

#View the status of BGP neighbors on Device 1.

```
Device1#show ip bgp summary
BGP router identifier 2.0.0.1, local AS number 100
BGP table version is 2
2 BGP AS-PATH entries
0 BGP community entries
```

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
1.0.0.2	4	200	2	2	2	0	0	00:01:32	1
2.0.0.2	4	200	2	2	2	0	0	00:01:43	1

#View the status of BGP neighbors on Device 2.

```
Device2#show ip bgp summary
BGP router identifier 20.0.0.1, local AS number 200
BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries

Neighbor    V  AS MsgRcvd MsgSent  TblVer  InQ  OutQ Up/Down  State/PfxRcd
1.0.0.1    4 100    2     2     2     0  0 00:02:52    0
30.0.0.1   4 200    3     3     2     0  0 00:02:45    1
```

It can be seen that BGP neighbor has been successfully established between Device1, Device2 and Device3.

#View the routing table of Device1.

```
Device1#show ip bgp
BGP table version is 3, local router ID is 1.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop        Metric LocPrf Weight Path
[B]* 3.0.0.0/24    2.0.0.2         50      0 200 i
[B]*> 1.0.0.2       0                0      0 200 i

Device1#show ip route bgp
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

B 3.0.0.0/24 [20/0] via 1.0.0.2, 00:07:19, vlan2
```

It can be seen that the route 3.0.0.0/24 on Device1 selects Device2 as the optimal next hop device.

Step 6: Configure coordination of BGP with BFD.

#Configure Device1.

```
Device1(config)#bfd fast-detect
Device1(config)#router bgp 100
Device1(config-bgp)#neighbor 1.0.0.2 fall-over bfd
Device1(config-bgp)#exit
Device1(config)#interface vlan2
Device1(config-if-vlan2)#bfd min-receive-interval 500
Device1(config-if-vlan2)#bfd min-transmit-interval 500
Device1(config-if-vlan2)#bfd multiplier 4
Device1(config-if-vlan2)#exit
```

#Configure Device2.

```
Device2(config)#bfd fast-detect
Device2(config)#router bgp 200
Device2(config-bgp)#neighbor 1.0.0.1 fall-over bfd
Device2(config-bgp)#exit
Device2(config)#interface vlan2
Device2(config-if-vlan2)#bfd min-receive-interval 500
Device2(config-if-vlan2)#bfd min-transmit-interval 500
Device2(config-if-vlan2)#bfd multiplier 4
Device2(config-if-vlan2)#exit
```

Enable BFD between EBGP neighbors Device1 and Device2, and modify BFD to control the minimum sending interval, minimum receiving interval and detection timeout multiples of packets.

Step 7: Check the result.

#View the BFD session status on Device1.

```
Device1#show bfd session
OurAddr      NeighAddr    LD/RD      State      Holddown    interface
1.0.0.1      1.0.0.2      2/2        UP         2000        vlan2
```

According to the result, BFD status on Device1 is correctly up, and the holddown time is negotiated as 2000ms.

#When the lines between Device1 and Device2 fail, the route can quickly switch to the backup line.

#View the routing table of Device1.

```
Device1#show ip bgp
BGP table version is 6, local router ID is 1.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop        Metric LocPrf Weight Path
[B]*> 3.0.0.0/24   2.0.0.2         50      0 200 i

Device1#show ip route bgp
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

B 3.0.0.0/24 [20/50] via 2.0.0.2, 00:00:05, vlan3
```

It can be seen that the next hop of 3.0.0.0/24 switches to Device3.

## 60.3.9 Configure BGP FRR

### Network Requirements

- All the devices are configured with BGP protocol.
- Device1 learns the BGP route 192.168.1.1/32 from Device2 and Device3 at the same time, and first uses the lines between it and Device3 to forward packets. Likewise, Device3 learns the BGP route 100.1.1.1/32 from Device1 and Device2, and prefers to use the lines between it and Device1 to forward packets.
- Enable BGP FRR on Device1 and Device3. When the lines between Device1 and Device3 fail, the service can quickly switch to Device2 for communication.

### Network Topology

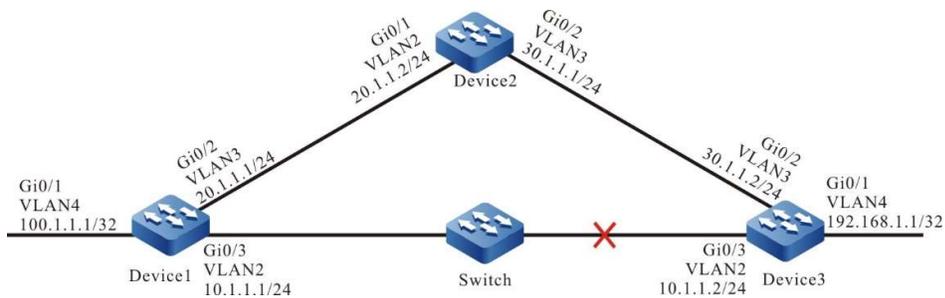


Figure 60 Network Topology for Configuring BGP FRR

### Configuration Steps

- Step 1: Configure VLAN, and add ports to the required VLAN; configure the IP address of each interface (Omitted).
- Step 2: Configure BGP.

Device1 establishes BGP neighbors with Device2 and Device3, and the route weight of neighbor with Device3 is 100.

```
Device1#configure terminal
Device1(config)#router bgp 100
Device1(config-bgp)#neighbor 10.1.1.2 remote-as 300
Device1(config-bgp)#neighbor 10.1.1.2 weight 100
Device1(config-bgp)#neighbor 20.1.1.2 remote-as 200
Device1(config-bgp)#network 100.1.1.1 255.255.255.255
Device1(config-bgp)#exit
```

#Device2 establishes BGP neighbors with Device1 and Device3.

```
Device2#configure terminal
Device2(config)#router bgp 200
Device2(config-bgp)#neighbor 20.1.1.1 remote-as 100
Device2(config-bgp)#neighbor 30.1.1.2 remote-as 300
Device2(config-bgp)#exit
```

#Device3 establishes BGP neighbors with Device1 and Device2, and the route weight of neighbor with Device1 is 100.

```
Device3#configure terminal
Device3(config)#router bgp 300
Device3(config-bgp)#neighbor 10.1.1.1 remote-as 100
Device3(config-bgp)#neighbor 10.1.1.1 weight 100
Device3(config-bgp)#neighbor 30.1.1.1 remote-as 200
Device3(config-bgp)#network 195.168.1.1 255.255.255.255
Device3(config-bgp)#exit
```

Step 3: Configure routing policy.

#On Device1, configure route-map to invoke ACL to match 192.168.1.1/32 only, and filter other networks.

The route matching the match rule applies the backup next hop address is 20.1.1.2.

```
Device1(config)#ip access-list standard 1
Device1(config-std-nacl)#permit 192.168.1.1 0.0.0.0
Device1(config-std-nacl)#exit
Device1(config)#route-map ipfir_bgp
Device1(config-route-map)#match ip address 1
Device1(config-route-map)#set fast-reroute backup-nexthop 20.1.1.2
Device1(config-route-map)#exit
```

#On Device3, configure route-map to invoke ACL to match 100.1.1.1/32 only, and filter other networks.

The route matching the match rule applies the backup next hop address is 30.1.1.1.

```
Device3(config)#ip access-list standard 1
Device3(config-std-nacl)#permit 100.1.1.1 0.0.0.0
Device3(config-std-nacl)#exit
Device3(config)#route-map ipfir_bgp
Device3(config-route-map)#match ip address 1
Device3(config-route-map)#set fast-reroute backup-nexthop 30.1.1.1
Device3(config-route-map)#exit
```

Step 4: Configure FRR.

#On Device1, enable BGP FRR.

```
Device1(config)#router bgp 100
Device1(config-bgp)#fast-reroute route-map ipfir_bgp
Device1(config-bgp)#exit
```

#On Device3, enable BGP FRR.

```
Device3(config)#router bgp 300
Device3(config-bgp)#fast-reroute route-map ipfir_bgp
Device3(config-bgp)#exit
```

Step 5: Check the result.

#View the routing table of Device1.

```
Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
C 10.1.1.0/24 is directly connected, 00:45:55, vlan2
L 10.1.1.1/32 is directly connected, 00:45:55, vlan2
C 20.1.1.0/24 is directly connected, 01:29:32, vlan3
L 20.1.1.1/32 is directly connected, 01:29:32, vlan3
```

```

C 127.0.0.0/8 is directly connected, 01:36:07, lo0
L 127.0.0.1/32 is directly connected, 01:36:07, lo0
LC 100.1.1.1/32 is directly connected, 01:35:18, vlan 4
B 192.168.1.1/32 [20/0] via 10.1.1.2, 00:04:40, vlan2

```

#The FRR table of Device1 shows the route of network 192.168.1.1/32. The next hop interface is vlan3.

```

Device1#show ip frr route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
B 192.168.1.1/32 [20/0] via 20.1.1.2, 00:00:02, vlan3

```

#According to the backup next hop information of Device1, the backup interface of FRR is vlan3.

```

Device1#show nexthop frr detail
Index          : 108
Type           : FRR
Reference Count : 1
Active Path    : master
Nexthop Address : 10.1.1.2
Interface      : vlan2
Interface Vrf  : global
Channel ID     : 19
Link Header Length : 18
Link Header    : 00017abc662b201201010101810000010800
Action        : FORWARDING
Slot          : 0
BK Nexthop Address : 20.1.1.2
BK Interface     : vlan3
BK Interface Vrf : global
BK Channel ID    : 20
BK Link Header Length : 18
BK Link Header   : 00017a455449201201010102810000020800
BK Action       : FORWARDING
BK Slot        : 0

```

Total 1 entries.

#When the lines between Device1 and Device3 fail, it will quickly identify the failures and switch to Device2 for communication. It can be seen from the routing table and FRR table of Device1 that the output interface of the destination network 192.168.1.1/32 in the routing table has switched to the backup interface vlan3.

```

Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
C 10.1.1.0/24 is directly connected, 00:45:55, vlan2
L 10.1.1.1/32 is directly connected, 00:45:55, vlan2
C 20.1.1.0/24 is directly connected, 01:29:32, vlan3
L 20.1.1.1/32 is directly connected, 01:29:32, vlan3
C 127.0.0.0/8 is directly connected, 01:36:07, lo0
L 127.0.0.1/32 is directly connected, 01:36:07, lo0
LC 100.1.1.1/32 is directly connected, 01:35:18, vlan 4
B 192.168.1.1/32 [20/0] via 20.1.1.2, 00:00:40, vlan3

```

On Device3, it is processed in a manner which is similar to that on Device1.

## 60.3.10 Configure basic functions of BGP-LS

### Network Requirements

- Device1 establishes OSPF neighbors with Device2 and advertises the route of the loopback interface to Device2.
- Device3 establishes OSPF neighbors with Device2, and advertises the route of the loopback interface to Device2.
- Device2 establishes BGP-LS neighbors with Device4, and advertises BGP-LS route to Device4.

### Network Topology

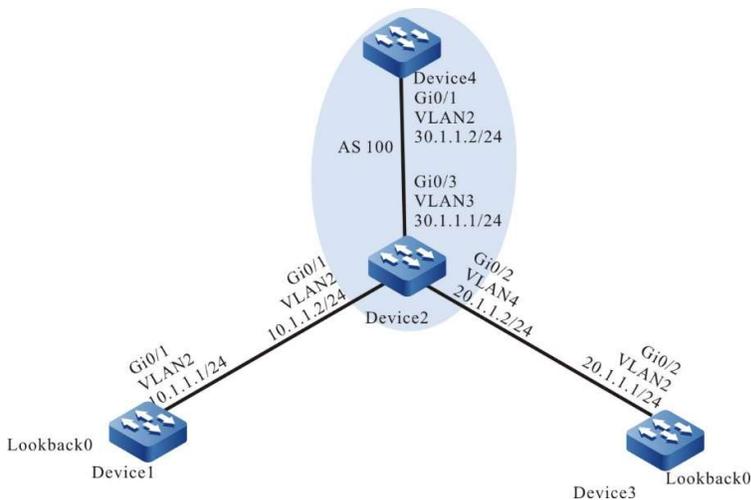


Figure 1 Network Topology for Configuring Basic Functions of BGP-LS

### Configuration Steps

Step 1: Configure VLAN, and add ports to the required VLAN; configure the IP address of each interface (Omitted).

Step 2: Configure OSPF.

#Device1 establishes OSPF neighbors with Device2 in backbone areas.

```
Device1#configure terminal
Device1(config)#router ospf 65535
Device1(config-ospf)#router-id 100.1.1.1
Device1(config-ospf)#network 10.1.1.0 0.0.0.255 area 0
Device1(config-ospf)#network 1.1.1.1 0.0.0.0 area 0
Device1(config-ospf)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 65535
Device2(config-ospf)#router-id 100.1.1.2
Device2(config-ospf)#network 10.1.1.0 0.0.0.255 area 0
Device2(config-ospf)#network 20.1.1.0 0.0.0.255 area 10
```

```
Device2(config-ospf)#exit
```

#Device3 establishes OSPF neighbors with Device2 in non-backbone areas.

```
Device3#configure terminal
Device3(config)#router ospf 65535
Device3(config-ospf)#router-id 100.1.1.3
Device2(config-ospf)#network 20.1.1.0 0.0.0.255 area 10
Device3(config-ospf)#network 3.3.3.3 0.0.0.0 area 10
Device3(config-ospf)#exit
```

Step 3: Configure BGP.

#Configure BGP on Device2 and activate the BGP-LS capability of the neighbors

```
Device2#configure terminal
Device2(config)#router bgp 65535
Device2(config-bgp)#bgp router-id 100.1.1.2
Device2(config-bgp)#neighbor 30.1.1.2 remote-as 65535
Device2(config-bgp)#address-family link-state unicast
Device2(config-bgp-af)#neighbor 30.1.1.2 activate
Device2(config-bgp-af)#exit-address-family
Device2(config-bgp)#exit
```

#Configure BGP on Device4 and activate the BGP-LS capability of the neighbors

```
Device4#configure terminal
Device4(config)#router bgp 65535
Device2(config-bgp)#bgp router-id 100.1.1.4
Device4(config-bgp)#neighbor 30.1.1.1 remote-as 65535
Device4(config-bgp)#address-family link-state unicast
Device4(config-bgp-af)#neighbor 30.1.1.1 activate
Device4(config-bgp-af)#exit-address-family
Device4(config-bgp)#exit
```

Step 4: Configure OSPF to import IGP topological information.

#Import IGP topological information under the OSPF address family of Device2.

```
Device1(config)#router ospf 65535
Device2(config-ospf)#distribute link-state
Device1(config-ospf)#exit
```

Step 5: Check the result.

#View the topological information of the IGP node generated by Device1.

```
Device2#show ip ospf 65535 link-state node
OSPF process 65535:
OSPF-LS local link state route:
Codes: N - Node route, L - Link route, P - Prefix route

N 100.1.1.1: [area:0.0.0.0] [DR:-] flags:0x0
N 100.1.1.2: [area:0.0.0.0] [DR:-] flags:0x10 ABR
N 100.1.1.2: [area:0.0.0.0] [DR:10.1.1.2] flags:0x10 ABR
N 100.1.1.2: [area:0.0.0.10] [DR:-] flags:0x10 ABR
N 100.1.1.3: [area:0.0.0.10] [DR:-] flags:0x0
N 100.1.1.3: [area:0.0.0.10] [DR:20.1.1.2] flags:0x0

Node route total number 6
```

#View the topological information of the IGP link generated by Device1.

```
Device2#show ip ospf 65535 link-state link
OSPF process 65535:
OSPF-LS local link state route:
Codes: N - Node route, L - Link route, P - Prefix route
```

```
L [100.1.1.1:10.1.1.1][100.1.1.2:10.1.1.2][area:0.0.0.0][DR:10.1.1.2] metric:1
L [100.1.1.2:10.1.1.2][100.1.1.1:10.1.1.1][area:0.0.0.0][DR:10.1.1.2] metric:1
L [100.1.1.2:10.1.1.2][100.1.1.2:10.1.1.2][area:0.0.0.0][DR:10.1.1.2] metric:1
L [100.1.1.2:10.1.1.2][100.1.1.2:10.1.1.2][area:0.0.0.0][DR:10.1.1.2] metric:1
L [100.1.1.2:20.1.1.1][100.1.1.3:20.1.1.2][area:0.0.0.10][DR:20.1.1.2] metric:1
L [100.1.1.3:20.1.1.2][100.1.1.2:20.1.1.1][area:0.0.0.10][DR:20.1.1.2] metric:1
L [100.1.1.3:20.1.1.2][100.1.1.3:20.1.1.2][area:0.0.0.10][DR:20.1.1.2] metric:1
L [100.1.1.3:20.1.1.2][100.1.1.3:20.1.1.2][area:0.0.0.10][DR:20.1.1.2] metric:1
```

Link route total number 8

### #View the topological information of the IGP prefix generated by Device1.

```
Device2#show ip ospf 65535 link-state prefix
OSPF process 65535:
OSPF-LS local link state route:
Codes: N - Node route, L - Link route, P - Prefix route
```

```
P 100.1.1.1:[1.1.1.1/32][area:0.0.0.0] type:1 Fwd:0.0.0.0 metric:1
P 100.1.1.1:[10.1.1.0/24][area:0.0.0.0] type:1 Fwd:0.0.0.0 metric:1
P 100.1.1.2:[10.1.1.0/24][area:0.0.0.0] type:1 Fwd:0.0.0.0 metric:1
P 100.1.1.2:[20.1.1.0/24][area:0.0.0.10] type:1 Fwd:0.0.0.0 metric:1
P 100.1.1.3:[3.3.3.3/32][area:0.0.0.10] type:1 Fwd:0.0.0.0 metric:1
P 100.1.1.3:[20.1.1.0/24][area:0.0.0.10] type:1 Fwd:0.0.0.0 metric:1
P 100.1.1.2:[3.3.3.3/32][area:0.0.0.0] type:2 Fwd:0.0.0.0 metric:2
P 100.1.1.2:[20.1.1.0/24][area:0.0.0.0] type:2 Fwd:0.0.0.0 metric:1
P 100.1.1.2:[1.1.1.1/32][area:0.0.0.10] type:2 Fwd:0.0.0.0 metric:2
P 100.1.1.2:[10.1.1.0/24][area:0.0.0.10] type:2 Fwd:0.0.0.0 metric:1
```

Prefix route total number 10

### #View the route of the BGP-LS node generated by Device1.

```
Device2#show bgp link-state unicast type node
BGP local router ID is 100.1.1.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Prefix codes: E link, V node, T IP reachable route, u/U unknown,
I Identifier, N local node, R remote node, L link, P prefix,
L1/L2 ISIS level-1/level-2, O OSPF, D direct, S static,
a area-ID, l link-ID, t topology-ID, s ISO-ID,
c confed-ID/ASN, b bgp-identifier, r router-ID,
i if-address, n nbr-address, o OSPF Route-type, p IP-prefix
d designated router address
```

```
Node Routes:
Network      Next Hop      Metric  LocPrf Weight Path
[O]*> [V][O][10x0][N[c65535][b100.1.1.2][a0.0.0.0][r100.1.1.1]]
          0.0.0.0      0        32768 i
[O]*> [V][O][10x0][N[c65535][b100.1.1.2][a0.0.0.0][r100.1.1.2]]
          0.0.0.0      0        32768 i
[O]*> [V][O][10x0][N[c65535][b100.1.1.2][a0.0.0.10][r100.1.1.2]]
          0.0.0.0      0        32768 i
[O]*> [V][O][10x0][N[c65535][b100.1.1.2][a0.0.0.10][r100.1.1.3]]
          0.0.0.0      0        32768 i
[O]*> [V][O][10x0][N[c65535][b100.1.1.2][a0.0.0.0][r100.1.1.2d10.1.1.2]]
          0.0.0.0      0        32768 i
[O]*> [V][O][10x0][N[c65535][b100.1.1.2][a0.0.0.10][r100.1.1.3d20.1.1.2]]
          0.0.0.0      0        32768 i
```

### #View the route of the BGP-LS link generated by Device1.

```
Device2#show bgp link-state unicast type link
BGP local router ID is 100.1.1.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
S Stale
```

Origin codes: i - IGP, e - EGP, ? - incomplete  
 Prefix codes: E link, V node, T IP reachable route, u/U unknown,  
 I Identifier, N local node, R remote node, L link, P prefix,  
 L1/L2 ISIS level-1/level-2, O OSPF, D direct, S static,  
 a area-ID, l link-ID, t topology-ID, s ISO-ID,  
 c confed-ID/ASN, b bgp-identifier, r router-ID,  
 i if-address, n nbr-address, o OSPF Route-type, p IP-prefix  
 d designated router address

Link Routes:

Network	Next Hop	Metric	LocPrf	Weight	Path
[O]*>					
[E][O][I0x0][N[c65535][b100.1.1.2][a0.0.0.0][r100.1.1.1]][R[c65535][b100.1.1.2][a0.0.0.0][r100.1.1.2d10.1.1.2]][L[i10.1.1.1][n10.1.1.2]]	0.0.0.0	0	32768	i	
[O]*>					
[E][O][I0x0][N[c65535][b100.1.1.2][a0.0.0.0][r100.1.1.2]][R[c65535][b100.1.1.2][a0.0.0.0][r100.1.1.2d10.1.1.2]][L[i10.1.1.2][n10.1.1.2]]	0.0.0.0	0	32768	i	
[O]*>					
[E][O][I0x0][N[c65535][b100.1.1.2][a0.0.0.10][r100.1.1.2]][R[c65535][b100.1.1.2][a0.0.0.10][r100.1.1.3d20.1.1.2]][L[i20.1.1.1][n20.1.1.2]]	0.0.0.0	0	32768	i	
[O]*>					
[E][O][I0x0][N[c65535][b100.1.1.2][a0.0.0.10][r100.1.1.3]][R[c65535][b100.1.1.2][a0.0.0.10][r100.1.1.3d20.1.1.2]][L[i20.1.1.2][n20.1.1.2]]	0.0.0.0	0	32768	i	
[O]*>					
[E][O][I0x0][N[c65535][b100.1.1.2][a0.0.0.0][r100.1.1.2d10.1.1.2]][R[c65535][b100.1.1.2][a0.0.0.0][r100.1.1.1]][L[i10.1.1.2][n10.1.1.1]]	0.0.0.0	0	32768	i	
[O]*>					
[E][O][I0x0][N[c65535][b100.1.1.2][a0.0.0.0][r100.1.1.2d10.1.1.2]][R[c65535][b100.1.1.2][a0.0.0.0][r100.1.1.2]][L[i10.1.1.2][n10.1.1.2]]	0.0.0.0	0	32768	i	
[O]*>					
[E][O][I0x0][N[c65535][b100.1.1.2][a0.0.0.10][r100.1.1.3d20.1.1.2]][R[c65535][b100.1.1.2][a0.0.0.10][r100.1.1.2]][L[i20.1.1.2][n20.1.1.1]]	0.0.0.0	0	32768	i	
[O]*>					
[E][O][I0x0][N[c65535][b100.1.1.2][a0.0.0.10][r100.1.1.3d20.1.1.2]][R[c65535][b100.1.1.2][a0.0.0.10][r100.1.1.3]][L[i20.1.1.2][n20.1.1.2]]	0.0.0.0	0	32768	i	

Total number of prefixes 8

### #View the route of the BGP-LS prefix generated by Device1.

```
Device2#show bgp link-state unicast type prefix4
BGP local router ID is 100.1.1.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Prefix codes: E link, V node, T IP reachable route, u/U unknown,
               I Identifier, N local node, R remote node, L link, P prefix,
               L1/L2 ISIS level-1/level-2, O OSPF, D direct, S static,
               a area-ID, l link-ID, t topology-ID, s ISO-ID,
               c confed-ID/ASN, b bgp-identifier, r router-ID,
               i if-address, n nbr-address, o OSPF Route-type, p IP-prefix
               d designated router address
Prefix4 Routes:
  Network          Next Hop          Metric    LocPrf Weight Path
[O]*> [T][O][I0x0][N[c65535][b100.1.1.2][a0.0.0.0][r100.1.1.1]][P[o0x01][p10.1.1.0/24]]
      0.0.0.0        0                32768 i
[O]*> [T][O][I0x0][N[c65535][b100.1.1.2][a0.0.0.0][r100.1.1.1]][P[o0x01][p1.1.1.1/32]]
      0.0.0.0        0                32768 i
[O]*> [T][O][I0x0][N[c65535][b100.1.1.2][a0.0.0.0][r100.1.1.2]][P[o0x01][p10.1.1.0/24]]
      0.0.0.0        0                32768 i
[O]*> [T][O][I0x0][N[c65535][b100.1.1.2][a0.0.0.0][r100.1.1.2]][P[o0x02][p20.1.1.0/24]]
      0.0.0.0        0                32768 i
[O]*> [T][O][I0x0][N[c65535][b100.1.1.2][a0.0.0.0][r100.1.1.2]][P[o0x02][p3.3.3.3/32]]
      0.0.0.0        0                32768 i
```

```

[O]*> [T][O][10x0][N[c65535][b100.1.1.2][a0.0.0.10][r100.1.1.2]][P[o0x01][p20.1.1.0/24]]
0.0.0.0      0      32768 i
[O]*> [T][O][10x0][N[c65535][b100.1.1.2][a0.0.0.10][r100.1.1.2]][P[o0x02][p10.1.1.0/24]]
0.0.0.0      0      32768 i
[O]*> [T][O][10x0][N[c65535][b100.1.1.2][a0.0.0.10][r100.1.1.2]][P[o0x02][p1.1.1.1/32]]
0.0.0.0      0      32768 i
[O]*> [T][O][10x0][N[c65535][b100.1.1.2][a0.0.0.10][r100.1.1.3]][P[o0x01][p20.1.1.0/24]]
0.0.0.0      0      32768 i
[O]*> [T][O][10x0][N[c65535][b100.1.1.2][a0.0.0.10][r100.1.1.3]][P[o0x01][p3.3.3.3/32]]
0.0.0.0      0      32768 i

```

Total number of prefixes 10

## #View the BGP-LS route received from Device2 on Device4

```

Device4#show bgp link-state unicast all-type
BGP local router ID is 100.1.1.4
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Prefix codes: E link, V node, T IP reachable route, u/U unknown,
              I Identifier, N local node, R remote node, L link, P prefix,
              L1/L2 ISIS level-1/level-2, O OSPF, D direct, S static,
              a area-ID, l link-ID, t topology-ID, s ISO-ID,
              c confed-ID/ASN, b bgp-identifier, r router-ID,
              i if-address, n nbr-address, o OSPF Route-type, p IP-prefix
              d designated router address
Node Routes:
  Network      Next Hop      Metric  LocPrf Weight Path
[B]*>i[V][O][10x0][N[c65535][b100.1.1.2][a0.0.0.0][r100.1.1.1]]
30.1.1.1      0      100  0 i
[B]*>i[V][O][10x0][N[c65535][b100.1.1.2][a0.0.0.0][r100.1.1.2]]
30.1.1.1      0      100  0 i
[B]*>i[V][O][10x0][N[c65535][b100.1.1.2][a0.0.0.10][r100.1.1.2]]
30.1.1.1      0      100  0 i
[B]*>i[V][O][10x0][N[c65535][b100.1.1.2][a0.0.0.10][r100.1.1.3]]
30.1.1.1      0      100  0 i
[B]*>i[V][O][10x0][N[c65535][b100.1.1.2][a0.0.0.0][r100.1.1.2d10.1.1.2]]
30.1.1.1      0      100  0 i
[B]*>i[V][O][10x0][N[c65535][b100.1.1.2][a0.0.0.10][r100.1.1.3d20.1.1.2]]
30.1.1.1      0      100  0 i
Link Routes:
  Network      Next Hop      Metric  LocPrf Weight Path
[B]*>i[E][O][10x0][N[c65535][b100.1.1.2][a0.0.0.0][r100.1.1.1]][R[c65535][b100.1.1.2][a0.0.0.0][r100.1.1.2d10.1.1.2]][L[i10
.1.1.1][n10.1.1.2]]
30.1.1.1      0      100  0 i
[B]*>i[E][O][10x0][N[c65535][b100.1.1.2][a0.0.0.0][r100.1.1.2]][R[c65535][b100.1.1.2][a0.0.0.0][r100.1.1.2d10.1.1.2]][L[i10
.1.1.2][n10.1.1.2]]
30.1.1.1      0      100  0 i
[B]*>i[E][O][10x0][N[c65535][b100.1.1.2][a0.0.0.10][r100.1.1.2]][R[c65535][b100.1.1.2][a0.0.0.10][r100.1.1.3d20.1.1.2]][L[i
20.1.1.1][n20.1.1.2]]
30.1.1.1      0      100  0 i
[B]*>i[E][O][10x0][N[c65535][b100.1.1.2][a0.0.0.10][r100.1.1.3]][R[c65535][b100.1.1.2][a0.0.0.10][r100.1.1.3d20.1.1.2]][L[i
20.1.1.2][n20.1.1.2]]
30.1.1.1      0      100  0 i
[B]*>i[E][O][10x0][N[c65535][b100.1.1.2][a0.0.0.0][r100.1.1.2d10.1.1.2]][R[c65535][b100.1.1.2][a0.0.0.0][r100.1.1.1]][L[i10
.1.1.2][n10.1.1.1]]
30.1.1.1      0      100  0 i
[B]*>i[E][O][10x0][N[c65535][b100.1.1.2][a0.0.0.0][r100.1.1.2d10.1.1.2]][R[c65535][b100.1.1.2][a0.0.0.0][r100.1.1.2]][L[i10
.1.1.2][n10.1.1.2]]
30.1.1.1      0      100  0 i
[B]*>i[E][O][10x0][N[c65535][b100.1.1.2][a0.0.0.10][r100.1.1.3d20.1.1.2]][R[c65535][b100.1.1.2][a0.0.0.10][r100.1.1.2]][L[i
20.1.1.2][n20.1.1.1]]
30.1.1.1      0      100  0 i
[B]*>i[E][O][10x0][N[c65535][b100.1.1.2][a0.0.0.10][r100.1.1.3d20.1.1.2]][R[c65535][b100.1.1.2][a0.0.0.10][r100.1.1.3]][L[i
20.1.1.2][n20.1.1.2]]
30.1.1.1      0      100  0 i
Prefix4 Routes:
  Network      Next Hop      Metric  LocPrf Weight Path
[B]*>i[T][O][10x0][N[c65535][b100.1.1.2][a0.0.0.0][r100.1.1.1]][P[o0x01][p10.1.1.0/24]]
30.1.1.1      0      100  0 i

```

```

[B]*>i[T][O][I0x0][N[c65535][b100.1.1.2][a0.0.0.0][r100.1.1.1]][P[o0x01][p1.1.1.1/32]]
30.1.1.1      0      100      0 i
[B]*>i[T][O][I0x0][N[c65535][b100.1.1.2][a0.0.0.0][r100.1.1.2]][P[o0x01][p10.1.1.0/24]]
30.1.1.1      0      100      0 i
[B]*>i[T][O][I0x0][N[c65535][b100.1.1.2][a0.0.0.0][r100.1.1.2]][P[o0x02][p20.1.1.0/24]]
30.1.1.1      0      100      0 i
[B]*>i[T][O][I0x0][N[c65535][b100.1.1.2][a0.0.0.0][r100.1.1.2]][P[o0x02][p3.3.3.3/32]]
30.1.1.1      0      100      0 i
[B]*>i[T][O][I0x0][N[c65535][b100.1.1.2][a0.0.0.10][r100.1.1.2]][P[o0x01][p20.1.1.0/24]]
30.1.1.1      0      100      0 i
[B]*>i[T][O][I0x0][N[c65535][b100.1.1.2][a0.0.0.10][r100.1.1.2]][P[o0x02][p10.1.1.0/24]]
30.1.1.1      0      100      0 i
[B]*>i[T][O][I0x0][N[c65535][b100.1.1.2][a0.0.0.10][r100.1.1.2]][P[o0x02][p1.1.1.1/32]]
30.1.1.1      0      100      0 i
[B]*>i[T][O][I0x0][N[c65535][b100.1.1.2][a0.0.0.10][r100.1.1.3]][P[o0x01][p20.1.1.0/24]]
30.1.1.1      0      100      0 i
[B]*>i[T][O][I0x0][N[c65535][b100.1.1.2][a0.0.0.10][r100.1.1.3]][P[o0x01][p3.3.3.3/32]]
30.1.1.1      0      100      0 i

```

Total number of prefixes 2

# 61 IPv6 BGP

---

## 61.1 Overview

IPv6 BGP (BGP4+) is an extension of BGP-4. BGP-4 can manage IPv4 routing information only. In order to support IPv6 protocol, IETF extends BGP-4 to form IPv6 BGP. Current IPv6 BGP standard is RFC 2858 (Multiprotocol Extensions for BGP-4).

IPv6 BGP needs to reflect the information of IPv6 network layer protocol in NLRI (Network Layer Reachability Information) and NEXT\_HOP attributes. The two NLRI attributes imported to IPv6 BGP are shown as follows:

- MP\_REACH\_NLRI: Multiprotocol Reachable NLRI. It can be used to distribute reachable route and next hop information.
- MP\_UNREACH\_NLRI: Multiprotocol Unreachable NLRI. It can be used to withdraw unreachable routes.

The NEXT\_HOP attribute in IPv6 BGP is represented by IPv6 address, either IPv6 global unicast address or link-local address.

IPv6 BGP utilizes the multi-protocol extension attribute of BGP for application in IPv6 networks. The original message mechanism and routing mechanism of BGP protocol have not changed.

## 61.2 IPv6 BGP function configuration

Table 61 BGP Function Configuration List

Configuration Task	
Configure IPv6 BGP Neighbor	Configure IBGP Neighbor
	Configure EBGP Neighbor
	Configure Passive BGP Neighbor
	Configure MP-BGP Neighbor
	Configure MD5 Authentication of BGP Neighbor
Configure BGP Route Generation	Configure BGP to Distribute Local Route
	Configure BGP Route Redistribution
	Configure BGP to Distribute Default Route
Configure BGP Route Control	Configure BGP to Distribute Aggregated Route
	Configure Administrative Distance of BGP Route
	Configure Routing Policy of BGP Neighbors in Outgoing Direction
	Configure Routing Policy of BGP Neighbors in Incoming Direction
	Configure the Maximum Number of Routing Entries Received by BGP Neighbors
	Configure the Maximum Number of BGP Load Balancing Entries
Configure BGP Route Attributes	Configure BGP Route Weight
	Configure MED Attributes of BGP Route
	Configure Local-Preference Attributes of BGP Route
	Configure AS_PATH Attributes of BGP Route

Configuration Task	
	Configure NEXT-HOP Attributes of BGP Route
	Configure Community Attributes of BGP Route
Configure BGP Network Optimization	Configure Keepalive Time of BGP Neighbor
	Configure BGP Route Detection Time
	Configure Fast Disconnection of EBGP Neighbor
	Configure BGP Route Dampening Function
	Configure BGP Neighbor Refresh Capability
	Configure Soft Resetting Capability of BGP Neighbor
	Configure ORF Capability of BGP Neighbor
Configure Large BGP Network	Configure BGP Peer Group
	Configure BGP Route Reflector
	Configure BGP Confederation
Configure BGP GR	Configure BGP GR Restarter
	Configure BGP GR Helper
Configure BGP to Coordinate with BFD	Configure EBGP to Coordinate with BFD
	Configure IBGP to Coordinate with BFD

### 61.2.1 Configure IPv6 BGP Neighbor

#### Configuration Condition

Before configuring BGP neighbors, do the following:

- The link layer protocol has been configured to ensure normal communication at the link layer.
- Configure address of interface at network layer so that neighbor network nodes are reachable at the network layer.

#### Configure IBGP Neighbor

## 1. Basic configuration

To configure IBGP neighbor, you are required to specify the same AS of neighbor as that of this device. Router ID can be configured for the device. It is used to uniquely mark a BGP device when establishing BGP session. When Router ID is not configured, the device will select one based interface address according to by following principles:

- Firstly, select the largest IP address from the Loopback interface as Router ID;
- If no Loopback interface is configured for IP address, select the largest IP addresses from other interfaces as Router ID;
- Only when the interface is UP can the interface address be selected as Router ID.

Table 61 Configuring IBGP Neighbor

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable the BGP protocol and enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	Mandatory By default, BGP is disabled.
Configure BGP device ID	<b>bgp router-id</b> <i>router-id</i>	Optional By default, the device makes selections according to interface address. In particular, Loopback interface and large IP address have a higher priority.
Configure IBGP Neighbor	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>remote-as</b> <i>as-number</i>	Mandatory By default, no IBGP neighbor is created.
Description of configuring IBGP neighbor	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>description</b> <i>description-string</i>	Optional By default, there is no description of IBGP neighbor.
Enter the BGP IPv6 unicast configuration mode	<b>address-family ipv6 unicast</b>	-

Step	Command	Description
Activate IBGP neighbor's capability of receiving and sending IPv6 unicast route	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>activate</b>	Optional By default, IBGP neighbor's capability of receiving and sending IPv6 unicast route is disabled.

## 2. Configure source address of TCP session

BGP uses TCP as transmission protocol. Featured by reliable transmission, TCP can effectively ensure that BGP protocol packets are correctly transmitted to the neighbors.

Table 61 Configuring Source Address of TCP Session

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable the BGP protocol and enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Configure IBGP Neighbor	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>remote-as</b> <i>as-number</i>	Mandatory By default, no IBGP neighbor is created.
Configure source address for TCP session of IBGP neighbors	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>update-source</b> { <i>interface-name</i>   <i>ipv6-address</i> }	Mandatory By default, the TCP session automatically selects the address of the route's output interface as source address.

### Note

- When there is load balancing route, source address of TCP session is required to be configured between BGP neighbors. When the TCP source address is not configured, different output interfaces may be used as their source addresses because neighbors have different optimal routes. As a result, BGP session cannot be successfully established within a period of time.

## Configure EBGP Neighbor

### 1. Basic configuration

To configure EBGP neighbor, you are required to specify different AS of neighbor from that of this device.

Table 61 Configuring EBGP Neighbor

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable the BGP protocol and enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Configure EBGP Neighbor	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>remote-as</b> <i>as-number</i>	Mandatory By default, no EBGP neighbor is created.

### 2. Configure Indirect EBGP Neighbor

Located in different operation networks, EBGP neighbors are often connected via a direct physical link. Thus, the default TTL value of IP packets communicated between EBGP neighbors is 1. If they are in the indirect operation network, you can set the TTL value of IP packets via a configuration command to allow BGP connection.

Table 61 Configuring Indirect EBGP Neighbor

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Configure EBGP Neighbor	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>remote-as</b> <i>as-number</i>	Mandatory By default, no EBGP neighbor is created.
Configure source address for TCP session of EBGP neighbors	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>update-source</b> { <i>interface-name</i>   <i>ipv6-address</i> }	Optional By default, the TCP session automatically selects the address of the route's output

Step	Command	Description
		interface as source address.
allow connection between indirect EBGP neighbors	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>ebgp-multihop</b> [ <i>tvl-value</i> ]	Mandatory By default, EBGP neighbor relation between indirect devices is not allowed.

### Configure Passive BGP Neighbor

The passive neighbor function is required in the special application environment. After passive neighbor is applied, BGP will not actively initiate a TCP connection request to establish BGP neighbor. The neighbor relation cannot be built until the neighbor actively issues a connection request. By default, the two neighbors will actively initiate connections to each other. When there is a conflict between the connections, a TCP connection will be selected to create a BGP session. Before configuring passive BGP neighbors, you need to configure BGP neighbors.

Table 61 Configuring Passive BGP Neighbor

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Configure BGP Neighbor	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>remote-as</b> <i>as-number</i>	Mandatory By default, no BGP neighbor is created.
Configure Passive BGP Neighbor	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>passive</b>	Mandatory By default, no passive neighbor is enabled.

### Configure MP-BGP Neighbor

By default, BGP neighbors cannot receive and send corresponding routes until activated in the VRF and VPN address family. Before configuring MP-BGP neighbors, you need to configure BGP neighbors.

Table 61 Configuring MP-BGP Neighbor

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Configure BGP Neighbor	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>remote-as</b> <i>as-number</i>	Mandatory By default, no BGP neighbor is created.
Enter the BGP IPv6 VRF configuration mode	<b>address-family ipv6 vrf</b> <i>vrf-name</i>	-
Configure neighbors under BGP IPv6 VRF address family	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>remote-as</b> <i>as-number</i>	Mandatory By default, no BGP neighbor is created.
Activate neighbors under IPv6 VRF address family	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>activate</b>	Optional By default, the neighbors under BGP IPv6 VRF configuration mode have been activated.
Exit the BGP IPv6 VRF configuration mode	<b>exit-address-family</b>	-

---

## Note

- Neighbors configured in BGP configuration mode and BGP IPv6 unicast configuration mode are global neighbors, and those configured in BGP IPv6 VRF configuration mode belong to the VRF address family only.
- 

### Configure MD5 Authentication of BGP Neighbor

BGP supports the configuration of MD5 authentication so as to protect the information exchange between neighbors. MD5 authentication is completed by TCP transmission protocol. To establish TCP connection, both neighbors must be configured with the same MD5 authentication password. Otherwise, TCP connection cannot be established after the TCP transmission protocol fails in MD5 authentication. Before configuring MD5 authentication for BGP neighbors, you need to configure BGP neighbors.

Table 61 Configuring MD5 Authentication for BGP Neighbor

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Configure BGP Neighbor	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>remote-as</b> <i>as-number</i>	Mandatory By default, no BGP neighbor is created.
Configure MD5 Authentication of BGP Neighbor	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>password</b> [ 0   7 ] <i>password-string</i>	Mandatory By default, there is no MD5 authentication between BGP neighbors.

## 61.2.2 Configure IPv6 BGP route generation

### Configuration Condition

Before configuring BGP route generation, ensure that:

- Enable BGP protocol.
- Configure IPv6 BGP neighbor and successfully establish and connect a session.

### Configure BGP to Distribute Local Route

BGP can import route from IPv6 routing table into BGP routing table through the **network** command. Only when there is an entry in the IPv6 routing table that fully matches the **network** prefix and mask, will the route be imported into the BGP routing table and distributed.

When distributing locate routes, you can apply a routing map for the routes or specify such routes as backdoor routes. Backdoor route deems EBGP route as local BGP route and uses the administrative distance of local route. In this case, IGP route is allowed to precede EBGP route, and the backdoor route will not advertise it to EBGP neighbors.

Table 61 Configuring BGP to Distribute Local Route

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Enter the BGP IPv6 unicast configuration mode	<b>address-family ipv6 unicast</b>	-
Configure BGP to Distribute Local Route	<b>network</b> <i>ipv6-prefix</i> [ <b>route-map</b> <i>rtmap-name</i> [ <b>backdoor</b> ]   <b>backdoor</b> ]	Mandatory By default, BGP doesn't distribute any local route.

## Note

- The Origin attribute of of the local route distributed by BGP is IGP.
- After using the `network backdoor` command on EBGp routes, the EBGp route administrative distance will become the local route administrative distance (by default, the EBGp route administrative distance is 20, and the local route administrative distance is 200), which is lower than the default IGP route administrative distance. In this case, the IGP route will be preferred, and a backdoor link will be created between EBGp neighbors.
- When BGP distributes local routes and applies the routing map, the match options supported include `as-path`, `community`, `extcommunity`, `ipv6 address`, `ipv6 nexthop`, and `metric`, and the set options supported include `as-path`, `comm-list`, `community`, `extcommunity`, `ipv6 next-hop`, `local-preference`, `metric`, `origin`, and `weight`.

### Configure BGP Route Redistribution

BGP is not responsible for learning routes. Instead, it focuses on controlling routing direction by managing route attributes. Therefore, BGP generates BGP routes for advertisement to neighbors by redistributing IGP. BGP can apply the routing map while redistributing IGP routes.

Table 1 Configuring BGP Route Redistribution

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-

Step	Command	Description
Enter the BGP IPv6 unicast configuration mode	<b>address-family ipv6 unicast</b>	-
Configure BGP to redistribute IGP routes	<b>redistribute</b> { <b>connected</b>   <b>isis</b> [ <i>area-tag</i> ] [ <b>match isis-level</b> ]   <b>ospf as-number</b> [ <b>match route-sub-type</b> ]   <b>rip process-id</b>   <b>static</b> } [ <b>route-map map-name</b> / <b>metric value</b> ]	Mandatory By default, BGP doesn't redistribute any other IGP routes.

## Note

- The Origin attribute of the IGP route distributed by BGP is INCOMPLETE.
- When BGP redistributes other protocols and applies the routing map, the match options supported include as-path, community, extcommunity, ipv6 address, ipv6 nexthop, and metric, and the set options supported include as-path, comm-list, community, extcommunity, ipv6 next-hop, local-preference, metric, origin, and weight.

### Configure BGP to Distribute Default Route

Before distributing a default route to neighbors, BGP is required to import a default route. This can be done by the following two manners: generate the default route of BGP via the command **neighbor default-originate**; redistribute the default route of other protocols via the command **default-information originate**.

The default route generated by the **neighbor default-originate** command is a route of 0::/0 automatically generated through BGP. The default route redistributed by the **default-information originate** command is a route of 0::/0 generated when BGP imports the redistributed protocol.

Table 61 Configuring BGP to Distribute Default Route

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Enter the BGP IPv6 unicast configuration mode	<b>address-family ipv6 unicast</b>	-

Step	Command	Description
Configure BGP to generate default route	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>default-originate</b> [ <b>route-map</b> <i>rtmap-name</i> ]	Mandatory By default, BGP doesn't generate default route.
Configure BGP to redistribute the default route of other protocols	<b>default-information originate</b>	Mandatory By default, BGP doesn't redistribute the default route of other protocols.

### Note

- When configuring BGP to redistribute the default route of other protocols, it is required to configure route redistribution.
- You can apply the routing map for the route when configuring BGP to generate a default route.
- When BGP generates default route and applies the routing map, the set options supported include as-path, comm-list, community, extcommunity, ipv6 next-hop, local-preference, metric, origin, and weight.

## 61.2.3 Configure IPv6 BGP route control

### Configuration Condition

Before configuring BGP route control, ensure that:

- Enable BGP protocol.
- Configure IPv6 BGP neighbor and successfully establish and connect a session.

### Configure BGP to Distribute Aggregated Route

In large BGP networks, in order to reduce the number of routes advertised to neighbors or effectively control the routing process of BGP, it is required to configure BGP aggregated route.

Table 61 Configuring BGP to Distribute Aggregated Route

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Enter the BGP IPv6 unicast configuration mode	<b>address-family ipv6 unicast</b>	-
Configure BGP to Distribute Aggregated Route	<b>aggregate-address</b> <i>ipv6-prefix</i> [ <b>as-set</b> / <b>summary-only</b> / <b>route-map</b> <i>rtmap-name</i> ]	Mandatory By default, route aggregation is disabled for BGP.

### Note

- When BGP distributes aggregated routes, the scale of route advertisement can be reduced by specifying the **summary-only** command option to advertise aggregated routes only.
- The aggregated route with AS\_PATH attribute can be generated by specifying the **as-set** command option.
- More attributes can be set for the aggregated routes by applying routing map to them.

### Configure Administrative Distance of BGP Route

Each protocol in the IP routing table has an administrative distance for routing control. The smaller the value, the higher the priority. BGP affects routing by configuring administrative distance for routes in the specified network segment. The administrative distances covered by the routes in the specified network segment will all be modified. At the same time, you may use ACL to effectively filter the network segment so that only the administrative distances in the network segment allowed by ACL can be modified.

The command **distance bgp** can be used to modify the administrative distance of BGP's external, internal and local routes, while the command **distance** is used to change that of the routes in the specified network segment. The command **distance** precedes **distance bgp**. The network segment configured to be covered by **distance** uses the administrative distance specified by this command, and that uncovered adopts the administrative distance set via **distance bgp**.

Table 2 Configuring BGP Route Administrative Distance

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Enter the BGP IPv6 unicast configuration mode	<b>address-family ipv6 unicast</b>	-
Configure BGP to modify the default administrative distance	<b>distance bgp</b> <i>external-distance internal-distance local-distance</i>	Optional By default, the administrative distance of EBGp route is 20, that of IBGP 200, and that of local route 200.
Configure administrative distance of the specified network segment	<b>distance administrative-distance</b> <i>ipv6-prefix [ acl-num   acl-name ]</i>	

### Configure Routing Policy of BGP Neighbors in Outgoing Direction

BGP route advertisement or routing relies on its powerful route attributes. When advertising routes to neighbors, you can modify route attributes or filter some routes by applying corresponding policies. Currently, the policies that can be applied in the outgoing direction include:

- distribute-list: distribution list;
- filter-list: filter list with AS\_PATH attribute;
- Prefix-list: IP prefix list;
- route-map: routing map.

Table 3 Configuring Routing Policy of BGP Neighbors in Outgoing Direction

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Enter the BGP IPv6 unicast configuration mode	<b>address-family ipv6 unicast</b>	-
Apply distribution list in the outgoing direction	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>distribute-list</b> { <i>access-list-num</i>   <i>access-list-name</i> } <b>out</b>	Multiple choice (distribution list and IP prefix list cannot be

Step	Command	Description
Apply the filter list with AS_PATH attribute in the outgoing direction	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>filter-list</b> <i>aspath-list-name</i> <b>out</b>	configured at the same time)  By default, the routing policy of BGP neighbors in the outgoing direction is not configured.
Apply IP prefix list in the outgoing direction	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>prefix-list</b> <i>prefix-list-name</i> <b>out</b>	
Apply routing map in the outgoing direction	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>route-map</b> <i>rtmap-name</i> <b>out</b>	

## Note

- After configuring the routing policy of BGP neighbors in the outgoing direction, it is required to reset the neighbors to make it take effect.
- When applying routing map in the outgoing direction of route reflector, only NEXT-HOP attribute can be changed.
- For the configuration of filter list, see the policy tools-configure AS-PATH list section.
- When configuring policy for neighbors in the outgoing direction, you can configure multiple policies at the same time. For BGP, the following sequence applies: distribute-list, filter-list, prefix-list, and route-map. After the first policy is rejected, the following policy will not be implemented. Only after all the policies configured pass will the routing information be advertised.
- For the routing map of BGP applied in outgoing direction, the match options supported include as-path, community, extcommunity, ipv6 address, ipv6 nexthop, and metric, and the set options supported include as-path, comm-list, community, extcommunity, ipv6 next-hop, local-preference, metric, origin, and weight.

### Configure Routing Policy of BGP Neighbors in Incoming Direction

BGP can use policies to filter the routing information received or modify its attributes. Like the outgoing direction, four policies are supported in the incoming direction:

- distribute-list: distribution list;
- filter-list: filter list with AS\_PATH attribute;
- Prefix-list: Configuring IPV6 prefix list;
- route-map: routing map.

Table 4 Configuring Application Policy of BGP Neighbors in Incoming Direction

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Enter the BGP IPv6 unicast configuration mode	<b>address-family ipv6 unicast</b>	-
Apply distribution list in the incoming direction	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>distribute-list</b> { <i>access-list-num</i>   <i>access-list-name</i> } <b>in</b>	Multiple choice (distribution list and IP prefix list cannot be configured at the same time)
Apply the filter list with AS_PATH attribute in the incoming direction	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>filter-list</b> <i>aspath-list-name</i> <b>in</b>	
Apply IP prefix list in the incoming direction	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>prefix-list</b> <i>prefix-list-name</i> <b>in</b>	By default, no policy is specified in the incoming direction.
Apply routing map in the incoming direction	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>route-map</b> <i>rtmap-name</i> <b>in</b>	

## Note

- After configuring the routing policy of BGP neighbors in the incoming direction, it is required to reset the neighbors to make it take effect.
- When configuring policy for neighbors in the incoming direction, you can configure multiple policies at the same time. For BGP, the following sequence applies: distribute-list, filter-list, prefix-list, and route-map. After the first policy is rejected, the following policy will not be implemented. Only after all the policies configured pass will the route be added to the database.
- For the routing policy of BGP applied in incoming direction, the match options supported include as-path, community, extcommunity, ipv6 address, ipv6 nexthop, and metric, and the set options supported include as-path, comm-list, community, extcommunity, ipv6 next-hop, local-preference, metric, origin, and weight.

### Configure the Maximum Number of Routing Entries Received by BGP Neighbors

For BGP device, you can limit the number of routing entries received from the designated neighbor. It gives alarms or disconnects when the routes received from the designated neighbor reaches a certain threshold.

Table 5 Configuring Maximum Number of Routing Entries Received by BGP Neighbors

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Enter the BGP IPv6 unicast configuration mode	<b>address-family ipv6 unicast</b>	-
Configure the maximum number of routing entries received by neighbors	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>maximum-prefix</b> <i>prefix-num</i> [ <i>threshold-value</i> ] [ <b>warning-only</b> ]	Mandatory By default, the number of prefix entries received from neighbors is not restricted.

### Note

- If the **warning-only** command option is not specified, the BGP session will be automatically disconnected when the number of routing entries received by BGP from the neighbor reaches the maximum.
- If the **warning-only** command option is specified, when the number of routing entries received by BGP from the neighbor reaches the maximum, only alarm message is given, and route learning continues.

### Configure the Maximum Number of BGP Load Balancing Entries

In the BGP networking environment, if there are several paths with the same cost to reach the same destination, you can achieve load balancing routing by configuring the number of BGP load entries.

Table 6 Configuring Maximum Number of Load Balancing Entries of BGP

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-

Step	Command	Description
Enter the BGP IPv6 unicast configuration mode	<b>address-family ipv6 unicast</b>	-
Configure the maximum number of IBGP load entries	<b>maximum-paths ibgp number</b>	Mandatory By default, there is no load balancing routing for IBGP.
Configure the maximum number of EBGP load entries	<b>maximum-paths number</b>	Mandatory By default, there is no load balancing routing for EBGP.

---

### Note

- After configuring the maximum number of EBGP load balancing entries, load can be formed only when EBGP route is preferred.
  - The commands used to configure the maximum number of load balancing entries vary with BGP configuration modes. For details, see the description of **maximum-paths** in BGP technical commands.
- 

## 61.2.4 Configure IPv6 BGP route attributes

### Configuration Condition

Before configuring BGP route attributes, ensure that:

- Enable BGP protocol.
- Configure IPv6 BGP neighbor and successfully establish and connect a session.

### Configure BGP Route Weight

The first rule for BGP routing is to compare the value of route weight. The larger the value, the higher the priority. The value of route weight is a local attribute of the device. It will not be transmitted to other BGP neighbors. It ranges from 0 to 65535. By default, the weight value of route learned from neighbors is 0, and those of all the routes generated on local device are 32768.

Table 7 Configuring BGP Route Weight

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Configure the route weight of neighbor or peer group	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>weight</b> <i>weight-num</i>	Mandatory By default, the route weight of neighbor is 0.

### Configure MED Attributes of BGP Route

MED attributes can be used to select the optimal route for the traffic entering AS. When other routing conditions are the same, if BGP learns the routes with the same destination address yet different next hops from different EBGP neighbors, it prefers that with the minimum MED value as the optimal entrance.

Sometimes MED is also called "external metric". It is marked as "metric" in the routing table of BGP. BGP will advertise the MED attributes of the routes learned from neighbors to IBGP neighbors rather than EBGP neighbors. Thus, MED is only applicable between neighboring AS.

#### 1. Configure BGP to allow comparison of MEDs from different AS neighboring routes

By default, BGP only performs MED routing for the routes learned from the same AS. You can use the **bgp always-compare-med** command to ignore the restriction on the same AS in MED routing.

Table 8 Configuring BGP to Allow Comparison of MEDs from Different AS Neighboring Routes

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Configure BGP to allow comparison of MEDs from different AS neighboring routes	<b>bgp always-compare-med</b>	Mandatory By default, BGP only allows to compare MEDs of the routes from the same AS

#### 2. Configure BGP to prioritise MEDs according to the route AS\_PATH-based group

By default, BGP doesn't prioritise MEDs according to the route AS\_PATH-based group. You can enable this function using the command **bgp deterministic-med**. When selecting routes, all routes are arranged based on AS\_PATH. Within each AS\_PATH group, the routes are ranked according to the MED size. The route with the minimum MED value is selected as the best route of this group.

Table 9 Configuring BGP to Prioritise MEDs According to the Route AS\_PATH-based Group

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
BGP prioritises MEDs according to the route AS_PATH-based group	<b>bgp deterministic-med</b>	Mandatory By default, BGP doesn't prioritise MEDs according to the route AS_PATH-based group.

### 3. Configure to compare MEDs of local confederated routes

By default, EBGP routes from different AS don't compare MED attributes. This principle also applies to the confederated EBGP. The command **bgp bestpath med confed** is used to enable comparison of MED attribute values for local confederated routes.

Table 10 Configuring BGP to Compare MEDs of Local Confederated Routes

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Configure BGP to compare MEDs of local confederated routes	<b>bgp bestpath med confed</b>	Mandatory By default, the MEDs of local confederated routes are not compared.

### 4. Configure the routing map to modify MED attributes

For route sending and receiving, routing map can be used to modify the value of MED attributes.

Table 11 Configuring Routing Map to Modify MED Attributes

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Enter the BGP IPv6 unicast configuration mode	<b>address-family ipv6 unicast</b>	-
Configure the routing map to modify MED attributes	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>route-map</b> <i>rtmap-name</i> <b>in</b>   <b>out</b>	Mandatory By default, routing map is not applied to any neighbor.

### Note

- When configuring the routing map to modify MED attributes, you are required to modify MED with the set metric command, see the policy tool-set metric.
- After the neighbor attribute-unchanged command is configured, MED attributes of the neighbor cannot be changed through routing map.

### Configure Local-Preference Attributes of BGP Route

Local-Preference attributes are transmitted among IBGP neighbors only. Local-Preference is used to select the optimal exit to leave AS. The route with the largest route will be preferred.

Its value ranges from 0 to 4294967295. The larger the value, the higher the priority. By default, all the routes advertised to IBGP neighbors have a Local-Preference attribute of 100, which can be modified through **bgp default local-preference** or routing map.

#### 1. Configure BGP to modify default Local-Preference attributes

Table 12 Configuring BGP to Modify Default Local-Preference Attributes

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Configure the default Local-Preference value	<b>bgp default local-preference</b> <i>local-value</i>	Optional By default, the local preference is 100.

## 2. Configure the routing map to modify Local- Preference attributes

Table 13 Configuring Routing Map to Modify Local-Preference Attributes

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Enter the BGP IPv6 unicast configuration mode	<b>address-family ipv6 unicast</b>	-
Configure the routing map to modify Local-Preference attributes	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>route-map</b> <i>rtmap-name</i> <b>in</b>   <b>out</b>	Mandatory By default, routing map is not applied to any neighbor.

### Note

- When configuring the routing map to modify Local-Preference attributes, you are required to modify Local-Preference attributes with the set local-preference command, see the policy tool-set local-preference.

## Configure AS\_PATH Attributes of BGP Route

### 1. Configure BGP to ignore comparison of AS\_PATH in routing

When other conditions are the same, BGP will prefer the route with the shortest AS\_PATH. You can cancel AS\_PATH routing via the command **bgp bestpath as-path ignore**.

Table 14 Configuring BGP to Ignore Comparison of AS\_PATH in Routing

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Configure BGP to ignore comparison of AS_PATH in routing	<b>bgp bestpath as-path ignore</b>	Mandatory By default, AS_PATH values are compared in routing.

## 2. Configure BGP for allowed Times of Repeated Local AS Number

In order to avoid routing loops, BGP will check the AS\_PATH attributes of the routes received from neighbors, and discard those containing local AS number. You may use the command **neighbor allowas-in** to allow the routes received by BGP to contain local AS number, and can configure the number of local AS numbers.

Table 15 Configuring BGP for allowed Times of Repeated Local AS Number

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Enter the BGP IPv6 unicast configuration mode	<b>address-family ipv6 unicast</b>	-
Configure to allow repeated local AS number	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>allowas-in</b> [ <i>as-num</i> ]	Mandatory By default, the AS_PATH attributes of the routes received from neighbors are not allowed to contain local AS number.

## 3. Configure BGP to remove private AS number when advertising route to neighbors

In large BGP networks, the AS\_PATH of routing has the following attributes: confederation or community. By default, BGP carries these private AS attributes when advertising to neighbors. In order to shield private network information, you can use **neighbor remove-private-AS** to remove private AS number.

Table 16 Configuring BGP to Remove Private AS Number When Advertising Route to Neighbors

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Enter the BGP IPv6 unicast configuration mode	<b>address-family ipv6 unicast</b>	-
Configure BGP to remove private AS number when advertising route to neighbors	<b>neighbor { neighbor-address   peer-group-name } remove-private-AS</b>	Mandatory By default, private AS number is carried when advertising to neighbors.

#### 4. Configure to detect legality of first AS number of EBG route

When BGP advertises route to EBG neighbors, the local AS number is pressed to the start position of AS\_PATH, and the first AS advertising this route will become the last one. Generally, the first AS number of the route received from EBG should be the same as the AS number of neighbors. Otherwise, this route will be discarded.

Table 17 Configuring to Detect Legality of First AS Number of EBG Route

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Configure to detect legality of the first AS number of EBG route	<b>bgp enforce-first-as</b>	Mandatory By default, the first AS number check mechanism is disabled in BGP.

## 5. Configure the routing map to modify AS\_PATH attributes

BGP supports the configuration of routing map to modify AS\_PATH attributes. You can add route attributes via **set as-path prepend** so as to affect the routing of neighbors. When using the function **set as-path prepend**, local AS is first used to add AS\_PATH. When using other AS, enough attention must be paid to avoid being rejected in route advertisement to this AS.

Table 18 Configuring Routing Map to Modify AS\_PATH Attributes

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Enter the BGP IPv6 unicast configuration mode	<b>address-family ipv6 unicast</b>	-
Configure the routing map to modify AS_PATH attributes	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>route-map</b> <i>rtmap-name</i> <b>in</b>   <b>out</b>	Mandatory By default, routing map is not applied to any neighbor.

### Note

- When configuring the routing map to modify AS\_PATH attributes, you are required to modify AS\_PATH attributes with the **set as-path prepend** command, see the policy tool-set **as-path**.

## Configure NEXT-HOP Attributes of BGP Route

When BGP advertises routes to IBGP neighbors, the route attributes (including next hop) are not changed. The next hop attribute is often used for BGP to advertise the routes learned by EBGP neighbors to IBGP neighbors. The **neighbor next-hop-self** command can be used to modify the next hop attribute of the routes advertised to BGP neighbors to use local IPv6 address. For BGP, you can also use routing map to modify the next hop attribute.

### 1. Configure BGP to use local IP address as next hop of route

Table 19 Configuring BGP to Use Local IP Address as Next Hop of Route

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Enter the BGP IPv6 unicast configuration mode	<b>address-family ipv6 unicast</b>	-
Configure to use local IP address as the next hop when advertising routes to neighbors	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>next-hop-self</b>	Mandatory  By default, the next hop attribute of the route advertised to EBGP neighbor is local IPv6 address. The next hop attribute of the route advertised to IBGP will not be modified. Its original attribute value will be kept unchanged.

## Note

- When configuring BGP to use local IPv6 address as the next hop of the route, if the source address of the TCP session is configured with the `neighbor update-source`, it will be used as the next hop address. Otherwise, the output interface address of the advertising device will be selected as local IPv6 address.

## 2. Configure the routing map to modify NEXT-HOP attributes

BGP supports the configuration of routing map to modify NEXT-HOP attributes through **set ipv6 next-hop**.

Table 20 Configuring Routing Map to Modify NEXT-HOP Attributes

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-

Step	Command	Description
Enter the BGP IPv6 unicast configuration mode	<b>address-family ipv6 unicast</b>	-
Configure the routing map to modify NEXT-HOP attributes	<b>neighbor { <i>neighbor-address</i>   <i>peer-group-name</i> } route-map <i>rtmap-name</i> in   out</b>	Mandatory By default, routing map is not applied to any neighbor.

---

### Note

- When configuring the routing map to modify NEXT-HOP attributes, you are required to modify these attributes with the `set ipv6 next-hop` command, see the `policy tool-set ipv6 next-hop`.
- 

## Configure Community Attributes of BGP Route

When advertising routes to neighbors, BGP allows the configuration of sending community attributes. You can apply routing map to match community attributes for specified neighbors in both incoming and outgoing directions.

Community attributes are used to identify a group of routes so as to apply routing policy to them. Community attributes have two forms, i.e. standard and extended. Standard community attributes have 4 bytes. Their attributes include NO\_EXPORT, LOCAL\_AS, NO\_ADVERTISE, and INTERNET. Extcommunity attributes have 8 bytes. Their attributes include Route Target (RT) and Route Origin.

### 1. Configure BGP to advertise community attributes of route to neighbors

**neighbor send-community** allows to advertise standard or extcommunity attributes or both to neighbors.

Table 21 Configuring BGP to Advertise Community Attributes of Route to Neighbors

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp <i>autonomous-system</i></b>	-
Enter the BGP IPv6 unicast configuration mode	<b>address-family ipv6 unicast</b>	-

Configure to advertise community attributes of route to neighbors	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>send-community</b> [ <b>both</b>   <b>extended</b>   <b>standard</b> ]	Mandatory By default, community attributes are not advertised to any neighbor.
---	--	---

## Note

- After the neighbor is activated under VPNv6 address family, the standard and extcommunity attributes will be automatically advertised to neighbors.

## 2. Configure the routing map to modify community attributes of route

BGP supports the configuration of routing map to modify community attributes through **set community**.

Table 22 Configuring Routing Map to Modify Community Attributes of Route

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Enter the BGP IPv6 unicast configuration mode	<b>address-family ipv6 unicast</b>	-
Configure the routing map to modify community attributes of BGP route	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>route-map</b> <i>rtmap-name</i> <b>in</b>   <b>out</b>	Mandatory By default, routing map is not applied to any neighbor.

## Note

- When configuring the routing map to modify community attributes of the route, you are required to modify community attributes with the **set community** command, see the **policy tool-set community**.

## 61.2.5 Configure IPv6 BGP network optimization

### Configuration Condition

Before configuring BGP network optimization, ensure that:

- Enable BGP protocol.
- Configure IPv6 BGP neighbor and successfully establish and connect a session.

### Configure Keepalive Time of BGP Neighbor

After a BGP session is successfully established, neighbors will periodically send Keepalive messages to maintain the BGP session relationship. If the neighbor's Keepalive message or route update packet is not received within the holdtime, the BGP session will be disconnected for over time. The keepalive time of the session will not be more than one third of the holdtime.

Table 23 Configuring Keepalive Time of BGP Neighbor

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Configure keepalive time and holdtime of global BGP	<b>timers bgp</b> <i>keepalive-interval holdtime-interval</i>	Optional
Configure the keepalive time and holdtime of BGP neighbor or peer group	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>timers</b> { <i>keepalive-interval holdtime-interval</i>   <b>connect</b> <i>connect-interval</i> }	By default, the interval of keepalive timer is 60 seconds; the interval of hold timer is 180 seconds; the interval of session reconnection timer is 120 seconds.

---

### Note

- The keepalive time and holdtime configured for specified neighbors precede those of global BGP.
  - After neighbor negotiation, the minimum holdtime will be used as the holdtime of BGP session.
  - When both keepalive time and holdtime are configured as zero, the neighbor keepalive/hold function is cancelled.
  - When the keepalive time interval is more than one third of the holdtime, the BGP session sends keepalive packets within one third of the holdtime.
-

## Configure BGP Route Detection Time

BGP mainly completes the pathfinding process with AS as the unit, and IGP completes the pathfinding process within the AS. Therefore, BGP routing often relies on IGP routing. After the next hop or output interface of IGP route on which BGP relies changes, BGP updates BGP route by periodically detecting IGP route. Update of local BGP route and other matters are completed within the detection period.

Table 24 Configuring BGP Route Detection Time

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Configure BGP Route Detection Time	<b>bgp scan-time</b> <i>time</i>	Optional By default, the BGP route detection time is 60 seconds.

---

### Caution

- When a very short BGP route detection time is configured, BGP will frequently detect routes. This will affect the performance of the device.
- 

## Configure Fast Disconnection of EBGP Neighbor

After a BGP session is successfully established, neighbors will periodically send Keepalive messages to each other to maintain the BGP session relationship. If the neighbor's Keepalive message or route update packet is not received within the holdtime, the BGP session will be disconnected for over time. You can configure a direct EBGP neighbor to disconnect BGP connection immediately when the connected interface is down, without waiting for the BGP keepalive timeout. When the fast disconnection of EBGP neighbors is cancelled, the EBGP session will not give a response to the down event on the interface. It will be disconnected after timeout.

Table 25 Configuring Fast Disconnection of EBGP Neighbor

Step	Command	Description
------	---------	-------------

Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Configure Fast Disconnection of EBGP Neighbor	<b>bgp fast-external-failover</b>	Optional By default, EBGP can give a fast response to the offline event on the direct interface.

### Configure BGP Route Dampening Function

Frequent route flapping in the network will make the network unstable. BGP suppresses such routes by configuring route dampening to reduce the impact of route flapping on the network.

For the routes subject to frequent flapping, their penalty value will increase. When the penalty value exceeds the dampening threshold, the route will not be advertised to neighbors. The penalty value shall not exceed the maximum dampening time. When no route flapping happens during the half-life, the penalty value will be halved. The route will not be re-advertised to neighbors until the value is less than the reuse limit.

- Half-life: The period when the penalty value of route is halved.
- Reuse limit: The limit that route returns to service.
- Suppress limit: The limit that the route is suppressed.
- Max suppress time: The maximum time that the route is suppressed.

Table 26 Configuring BGP Route Suppression Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Enter the BGP IPv6 unicast configuration mode	<b>address-family ipv6 unicast</b>	-
Configure BGP route dampening period	<b>bgp dampening</b> [ <i>reach-half-life</i> [ <i>reuse-value suppress-value max-suppress-time</i>	Mandatory

	[ <i>unreach-half-life</i> ] ]   <b>route-map</b> <i>rtmap-name</i> ]	By default, the route suppression function is disabled. After it is enabled, the default route suppression half-life is 15 minutes; the route reuse limit is 750; the route suppress limit is 2000; the max suppress time is 60 minutes; the unreachable half-life of route penalty is 15 minutes.
--	---	--

### Note

- Route flapping includes both addition or deletion of routes, and change of route attributes, such as next hop and MED attributes.

### Configure BGP Neighbor Refresh Capability

When the routing policy or route selection policy applied by BGP neighbors changes, the routing table needs to be refreshed again by two manners. One is to reset by recovering BGP connection to restart the session. This method may cause BGP route flapping and affect business operation. The other one is more graceful. You need to configure the BGP device of local port to support the capability of route refresh. When its neighbor needs to reset the route, the Route-Refresh message is sent to local port which will re-send the route to this neighbor after receiving the message. In this case, the routing table is dynamically refreshed without disconnecting BPG sessions.

Table 27 Configuring Refreshing Capability of BGP Neighbor

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Enable BGP Neighbor Refresh Capability	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>capability route-refresh</b>	Optional By default, advertising neighbors to support

Step	Command	Description
		route refresh capability is enabled.

### Configure Soft Resetting Capability of BGP Neighbor

When the routing policy or route selection policy applied by BGP neighbors changes, the routing table needs to be refreshed again by two manners. One is to reset by recovering BGP connection to restart the session. This method may cause BGP route flapping and affect business operation. Another more graceful method is to configure local BGP device to support route refresh capability. You can also enable the soft resetting capability of local BGP device. By default, the BGP device retains the routing information of all neighbors. After enabling its neighbors' soft reset capability, it refreshes the routes of local retained neighbors again. At this time, the BGP session will not be disconnected.

Table 28 Configuring Soft Resetting Capability of BGP Neighbor

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Enter the BGP IPv6 unicast configuration mode	<b>address-family ipv6 unicast</b>	-
Enable soft resetting capability of BGP neighbor	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>soft-reconfiguration inbound</b>	Mandatory By default, the soft resetting function is disabled.

### Configure ORF Capability of BGP Neighbor

BGP accurately controls routes through various route attributes. To this end, it usually applies routing policy in both incoming and outgoing directions, a local behavior of BGP. BGP also supports ORF (Outbound Route Filtering) capability. It advertises local ingress policy through Route-refresh packet to its neighbor which applies this policy when advertising routes to it. This can largely reduce the interactions of route update packet between BGP neighbors.

To successfully negotiate ORF capability, the following conditions must be satisfied:

- Both neighbors need to enable ORF capability;
- ORF send and ORF receive must be paired, i.e., if one uses ORF send, the other must be ORF both or ORF receive; if one uses ORF receive, the other must be ORF send or ORF both;

- For the neighbor using ORF send, a prefix list needs to be applied in the incoming direction.

Table 29 Configuring ORF Capability of BGP Neighbor

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Enter the BGP IPv6 unicast configuration mode	<b>address-family ipv6 unicast</b>	-
Make the neighbor apply prefix list in the incoming direction	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>prefix-list</b> <i>prefix-list-name</i> <b>in</b>	Mandatory By default, prefix list is not applied to any BGP neighbor.
Make the neighbor support ORF capability	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>capability orf prefix-list</b> { <b>both</b>   <b>receive</b>   <b>send</b> }	Mandatory By default, advertising neighbors to support ORF capability is disabled.

## 61.2.6 Configure large IPv6 BGP network

### Configuration Condition

Before configuring large BGP network, ensure that:

- Enable BGP protocol;
- Configure IPv6 BGP neighbor and successfully establish and connect a session.

### Configure BGP Peer Group

BGP peer group is a set of BGP neighbors with the same configuration policy. Any configuration of the peer group will influence all the members in the group. Configuring BGP peer group is beneficial for the centralized management and maintenance of neighbors.

Table 61 Configuring BGP Peer Group

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Enter the BGP IPv6 unicast configuration mode	<b>address-family ipv6 unicast</b>	-
Create BGP peer group	<b>neighbor</b> <i>peer-group-name</i> <b>peer-group</b>	Mandatory
Add neighbors into the peer group	<b>neighbor</b> <i>neighbor-address</i> <b>peer-group</b> <i>peer-group-name</i>	By default, peer group is not configured, and neighbors are not added into any peer group.

---

## Note

- The configuration of peer group will influence all the group members.
  - After a neighbor is added into the peer group, the configuration of the original one which is the same as that of the peer group will be deleted.
  - After configuring the routing policy in outgoing and incoming directions for the peer group, if the routing policy changes, it is not effective for the neighbor already added into the peer group. The altered routing policy cannot apply to members of the peer group until the peer group is reset.
- 

### Configure BGP Route Reflector

In large BGP networking environments, IBGP neighbors are required to be connected across the whole network. That is to say, each BGP has to connect with all the other IBGP neighbors. Then, in the networking environment with N BGP neighbors, there are  $N*(N-1)/2$  BGP connections. The more the connections, the larger the amount of route advertisement. BGP route reflector can reduce the number of network connections. It includes several IBGPs into a group, and specifies a BGP as a reflector (RR), other BGPs as clients, and the BGPs not in the group as non-clients. The clients establish peering relationships with the RR only to reduce necessary IBGP connections. The number of connections can be decreased to N-1.

The principle of reflecting routes by BGP route reflector:

- The routes learned from non-client IBGP neighbors are reflected to clients only;
- The routes learned from clients will be reflected to all the clients and non-clients except the clients initiating these routes;
- The routes learned from EBGP clients will be reflected to all the clients and non-clients.

Table 30 Configuring BGP Route Reflector

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Configure reflector cluster ID	<b>bgp cluster-id</b> { <i>cluster-id-in-ip</i>   <i>cluster-id-in-num</i> }	Mandatory By default, the route reflector cluster ID is the Router ID of the device.
Configure neighbor as reflector client	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>route-reflector-client</b>	Mandatory By default, no neighbor is specified as reflector client.
Configure the route reflection function between BGP clients	<b>bgp client-to-client reflection</b>	Optional By default, the route reflection function between BGP route reflector clients is enabled.

---

 **Note**

- Reflector cluster ID is used to identify the same reflector area with many reflectors that have the same reflector cluster ID.
- 

### Configure BGP Confederation

In large BGP networking environments, IBGP neighbors are required to be connected across the whole network. That is to say, each BGP has to connect with all the other IBGP neighbors. Then, in the networking environment with N BGP neighbors, there are  $N*(N-1)/2$  BGP connections. The more the connections, the larger the amount of route advertisement. BGP confederation can also reduce network connections. It uses the divide-and-conquer strategy to divide the AS into several sub-AS areas. Each of them forms a confederation which is fully connected through IBGP. The sub-AS areas of the confederation are connected via EBGP to effectively reduce BGP connections.

When configuring BGP confederation, it is required to assign a confederation ID to each confederation and specify members of such confederation. Unlike route reflector (only route reflector is required to support route reflection when necessary), confederation requires all members to support the confederation function.

Table 31 Configuring BGP Confederation

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Create BGP confederation ID	<b>bgp confederation identifier</b> <i>as-number</i>	Mandatory By default, no confederation AS number is configured.
Configure BGP confederation members	<b>bgp confederation peers</b> <i>as-number-list</i>	Mandatory By default, the confederation's sub-AS number is not configured.

---

 **Note**

- The confederation ID is used to identify the confederation sub-AS which contains the confederation members.
- 

### 61.2.7 Configure IPv6 BGP GR

GR (Graceful Restart) is used to keep the routing information in the forwarding layer of this device and neighbor device unchanged during the switch between host and standby devices to ensure the forwarding process is not affected; after the device is switched for re-running, the two devices synchronize routing information and update forwarding layer in the protocol layer so that the data can keep forwarding during the process of device switch.

Roles in GR process:

- GR Restarter: The device for graceful restart of protocol.

- GR Helper: The device which helps with the graceful restart of protocol.
- GR Time: The maximum time for GR-Restarter to restart. GR Helper maintains routing stability during this period of time only.

The dual-master device can act as GR Restarter and GR Helper, while the centralized device only serves as GR Helper to help the Restarter complete GR. When the GR Restarter is doing GR, GR Helper maintains its route until GR Time is time out and the GR is completed for routing information synchronization. During this period of time, network routing and packet forwarding stays at the status prior to GR, which effectively ensures network stability.

BGP GR relationship is established through OPEN packet negotiation when neighbors establish connections. When the GR Restarter neighbor restarts, the BGP session will be disconnected, but the routes learned from the neighbor will not be deleted. They will continue to be forwarded normally in the IP routing table. Marked with Stale in the BGP routing table, they will be updated after GR is completed or time out.

GR Restarter needs to complete the connection with GR Helper within the maximum allowable time (**restart-time**). Otherwise, GR Helper will eliminate the GR routes retained and cancel the GR process. After neighbor re-establishment is completed, the GR Helper needs to receive the update packets with End-Of-RIB tag from the GR Restarter to successfully complete the GR process. Otherwise, the GR route not updated will be deleted after the maximum hold time (**stalepath-time**), and the GR relationship will be cancelled.

### Configuration Condition

Before configuring BGP GR, ensure that:

- Enable BGP protocol.
- Configure IPv6 BGP neighbor and successfully establish and connect a session.

Configure BGP GR Restarter

Table 32 Configuring BGP GR Restarter

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Enable BGP GR capability	<b>bgp graceful-restart</b> [ <b>restart-time</b> <i>time</i>   <b>stalepath-time</b> <i>time</i> ]	Mandatory By default, the GR capability is not enabled on the BGP device. After GR is enabled, the default maximum

Step	Command	Description
		allowable time for neighbors to re-establish sessions is 120 seconds; the maximum hold time of GR routes is 360 seconds.
Enter the BGP IPv6 unicast configuration mode	<b>address-family ipv6 unicast</b>	-
Configure to advertise GR-Restarter capability to neighbors	<b>neighbor { <i>neighbor-address</i>   <i>peer-group-name</i> } capability graceful-restart</b>	Mandatory By default, GR-Restarter capability is not advertised to any neighbor.

### Configure BGP GR Helper

Table 33 Configuring BGP GR Helper

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp <i>autonomous-system</i></b>	-
Enable BGP GR capability	<b>bgp graceful-restart [ <i>restart-time time</i>   <i>stalepath-time time</i> ]</b>	Mandatory By default, the GR capability is not enabled on the BGP device. After GR is enabled, the default maximum allowable time for neighbors to re-establish sessions is 120 seconds; the maximum hold time of GR routes is 360 seconds.

## 61.2.8 Configure coordination of IPv6 BGP with BFD

Generally, there are other intermediate devices between BGP neighbors. When these devices fail, BGP sessions are normal within the hold time. They cannot give a response to the link failures of intermediate devices in a timely manner. BFD (Bidirectional Forwarding Detection) provides a method to quickly detect the status of lines between two devices. When BFD detection is enabled between BGP devices, if there is a line failure between the devices, BFD can quickly detect the failure and notify BGP to trigger BGP to rapidly disconnect the session and switch to the backup line. In this way, it can reach the purpose of fast route switch.

### Configuration Condition

Before configuring the coordination of BGP with BFD, ensure that:

- Enable BGP protocol.
- Configure IPv6 BGP neighbor and successfully establish and connect a session.

### Configure EBGP to Coordinate with BFD

The coordination of EBGP with BFD is based on single-hop BFD sessions, and BFD session parameters are required to be configured in interface mode.

Table 34 Configuring Coordination of EBGP with BFD

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Enter the BGP IPv6 unicast configuration mode	<b>address-family ipv6 unicast</b>	-
Configure EBGP to Coordinate with BFD	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>fall-over bfd</b> [ <b>single-hop</b> ]	Mandatory By default, the BFD function of neighbor is disabled.
Exit the BGP IPv6 unicast configuration mode	<b>exit-address-family</b>	-
Exit the BGP configuration mode	<b>exit</b>	-

Step	Command	Description
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure the minimum receiving time interval of BFD sessions	<b>bfd min-receive-interval</b> <i>milliseconds</i>	Optional By default, the minimum receiving time interval of BFD sessions is 1000 seconds.
Configure the minimum sending time interval of BFD sessions	<b>bfd min-transmit-interval</b> <i>milliseconds</i>	Optional By default, the minimum sending time interval of BFD sessions is 1000 seconds.
Configure the BFD session detection timeout multiple	<b>bfd multiplier</b> <i>number</i>	Optional The BFD session detection timeout multiple is 5.

---

### Note

- For the BFD-related configurations, please see the Reliability Technology - BFD-related section.
- 

### Configure IBGP to Coordinate with BFD

The coordination of IBGP with BFD is based on multi-hop BFD sessions, and BFD session parameters are required to be configured in BGP mode.

Table 35 Configuring Coordination of IBGP with BFD

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-

Step	Command	Description
Enter the BGP IPv6 unicast configuration mode	<b>address-family ipv6 unicast</b>	-
Configure IBGP to Coordinate with BFD	<b>neighbor { <i>neighbor-address</i>   <i>peer-group-name</i> } fall-over bfd [single-hop]</b>	Mandatory By default, the BFD function of neighbor is disabled.
Configure the minimum receiving time interval of BFD sessions	<b>bfd min-receive-interval <i>milliseconds</i></b>	Optional By default, the minimum receiving time interval of BFD sessions is 1000 seconds.
Configure the minimum sending time interval of BFD sessions	<b>bfd min-transmit-interval <i>milliseconds</i></b>	Optional By default, the minimum sending time interval of BFD sessions is 1000 seconds.
Configure the BFD session detection timeout multiple	<b>bfd multiplier <i>number</i></b>	Optional The BFD session detection timeout multiple is 5.

## 61.2.9 Configure IPv6 BGP FRR

### Configuration Condition

Before configuring IPv6 BGP FRR, ensure that:

- When the FRR based on route-map is configured, the associated route-map has been configured.
- Enable IPv6BGP protocol.

### Configure BGP FRR

In the IPv6BGP network, as a result of link or device failure, the packets passing the point of failure will be discarded or loops will be produced. The traffic interruption caused thereby will continue until the protocol reconverges after several seconds. IPv6BGP FRR can reduce the time of traffic interruption. By applying the routing map, set a backup next hop for the successfully matched route. Once the main link fails, the traffic

passing through the main link will immediately switch to the backup link, achieving the purpose of fast switching.

Table 36 Configuring IPv6 BGP FRR

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Enter the BGP IPv6 unicast configuration mode	<b>address-family ipv6 unicast</b>	-
Configure the route-map-based FRR of BGP	<b>fast-reroute route-map</b> <i>route-map-name</i>	Mandatory By default, the route-map FRR function is disabled.
Configure BGP auto FRR	<b>pic</b>	Mandatory By default, the BGP auto FRR function is disabled.

---

### Caution

- After BGP FRR is configured, BGP needs to be reset to complete initial route check and backup. Otherwise, it is only effective for the routes learned after the configuration.
  - When set fast-reroute backup-nexthop is configured for the FRR based on route-map, the protocol enables automatic FRR;
  - When pic method is used, the protocol enables automatic FRR;
  - The methods of enabling FRR are mutually exclusive;
  - After configuring BGP FRR and applying the routing map, use the command set backup-nexthop nexthop-address to set the BGP neighbor as the backup next hop in the routing map. If the non-BGP neighbor is configured as the backup next hop, the FRR function cannot take effect.
- 

## 61.2.10 IPv6 BGP monitoring and maintaining

Table 37 BGP Monitoring and Maintaining

Command	Description
<b>clear bgp ipv6</b> { *   <i>as-number</i>   <b>peer-group</b> <i>peer-group-name</i>   <b>external</b>   <i>neighbor-address</i> } [ <b>vrf</b> <i>vrf-name</i> ]	Reset BGP neighbors
<b>clear bgp</b> [ <b>ipv6 unicast</b> ] <b>dampening</b> [ <i>ipv6-address</i>   <i>ipv6-address/mask-length</i> ]	Clear dampened routes
<b>clear bgp</b> [ <b>ipv6 unicast</b> ] <b>flap-statistics</b> [ <i>ipv6-address</i>   <i>ipv6-address/mask-length</i> ]	Clear jitter statistics
<b>clear bgp</b> [ <b>ipv6</b> ] { *   <i>as-number</i>   <b>peer-group</b> <i>peer-group-name</i>   <b>external</b>   <i>neighbor-address</i> } [ <b>vrf</b> <i>vrf-name</i> ] { [ <b>soft</b> ] [ <b>in</b>   <b>out</b> ] }	Softly reset neighbors
<b>clear bgp</b> [ <b>ipv6</b> ] { *   <i>neighbor-address</i>   <i>as-number</i>   <b>peer-group</b> <i>peer-group-name</i>   <b>external</b> } [ <b>vrf</b> <i>vrf-name</i> ] <b>in prefix-filter</b>	Advertise ORF to neighbors
<b>show bgp</b> { <b>ipv6 unicast</b>   <b>vpnv6 unicast</b> <b>vrf</b> <i>vrf-name</i> } [ <i>ipv6-address</i>   <i>ipv6-address/mask-length</i> ]	Show the routing information under corresponding address family of BGP
<b>show ip bgp attribute-info</b>	Show the public route attributes of BGP
<b>show bgp ipv6 unicast community</b> [ <i>community-number</i> / <i>aa:nn</i> / <b>exact-match</b> / <b>local-AS</b> / <b>no-advertise</b> / <b>no-export</b> ]	Show the routing information which matches specified community attributes
<b>show bgp ipv6 unicast community-list</b> <i>community-list-name</i>	Show the community attribute list applied to routing information
<b>show bgp</b> { <b>ipv6 unicast</b>   <b>vpnv6 unicast</b> <b>vrf</b> <i>vrf-name</i> } <b>dampening</b> { <b>dampened-paths</b>   <b>flap-statistics</b>   <b>parameters</b> }	Show detailed information of route dampening
<b>show bgp ipv6 unicast filter-list</b> <i>filter-list-name</i> [ <b>exact-match</b> ]	Show the routes matching AS_PATH access list
<b>show bgp ipv6 unicast inconsistent-as</b>	Show the routes in conflict with AS_PATH

Command	Description
<b>show bgp { ipv6 unicast   vpv6 uicast vrf vrf-name } neighbors [ ipv6-address ]</b>	Show the detailed information BGP neighbors
<b>show bgp ipv6 unicast prefix-list prefix-list-name</b>	Show the routes matching prefix list
<b>show bgp ipv6 unicast quote-regexp as-path-list-name</b>	Show the routes matching AS_PATH list
<b>show bgp ipv6 unicast regexp as-path-list-name</b>	Show the routes matching AS_PATH list
<b>show bgp ipv6 unicast route-map rtmap-name</b>	Show the route matching the routing map
<b>show ip bgp scan</b>	Show the scanning information of BGP
<b>show bgp {ipv6 unicast   vpv6 vrf vrf-name } summary</b>	Show the neighbor summarization information of BGP

## 61.3 Typical configuration example of IPv6 BGP

### 61.3.1 Configure basic functions of IPv6 BGP

#### Network Requirements

- EBGP neighbors are established between Device1 and Device2, and IBGP neighbors are established between Device2 and Device3.
- Device1 learns the direct route 2001:4::/64 from the interface of Device3 which learns the direct route 2001:1::/64 from the interface of Device1.

#### Network Topology

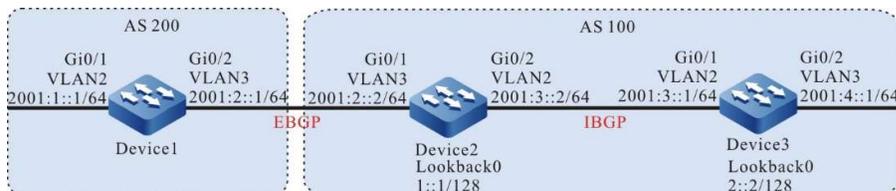


Figure 61 Network Topology for Configuring Basic Functions of IPv6 BGP

#### Configuration Steps

Step 1: Configure IPv6 global unicast address for interface. (Omitted)

Step 2: Configure OSPFv3 so that the routes of Loopback interfaces between devices are reachable from each other.

#### #Configure Device2.

```
Device2#configure terminal
Device2(config)#ipv6 router ospf 100
Device2(config-ospf6)#router-id 2.2.2.2
Device2(config-ospf6)#exit
Device2(config)#interface vlan 2
Device2(config-if-vlan2)#ipv6 router ospf 100 area 0
Device2(config-if-vlan2)#exit
Device2(config)#interface loopback 0
Device2(config-if-loopback0)#ipv6 router ospf 100 area 0
Device2(config-if-loopback0)#exit
```

#### #Configure Device3.

```
Device3#configure terminal
Device3(config)#ipv6 router ospf 100
Device3(config-ospf6)#router-id 3.3.3.3
Device3(config-ospf6)#exit
Device3(config)#interface vlan 2
Device3(config-if-vlan2)#ipv6 router ospf 100 area 0
Device3(config-if-vlan2)#exit
Device3(config)#interface loopback 0
Device3(config-if-loopback0)#ipv6 router ospf 100 area 0
Device3(config-if-loopback0)#exit
```

#### #View the routing table of Device 2.

```
Device2#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
  via ::, 1w1d:23:51:37, lo0
LC 1::1/128 [0/0]
  via ::, 00:09:34, loopback0
O 2::2/128 [110/2]
  via fe80::201:7aff:fec0:525a, 00:05:29, vlan2
C 2001:2::/64 [0/0]
  via ::, 00:09:41, vlan3
L 2001:2::2/128 [0/0]
  via ::, 00:09:39, vlan3
C 2001:3::/64 [0/0]
  via ::, 00:08:55, vlan2
L 2001:3::2/128 [0/0]
  via ::, 00:08:53, vlan2
```

#### #Check the routing table of Device3.

```
Device3#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
  via ::, 1w5d:18:34:53, lo0
O 1::1/128 [110/2]
  via fe80::201:7aff:fe5e:6d2e, 00:29:59, vlan2
```

```

LC 2::2/128 [0/0]
  via ::, 00:32:36, loopback0
C 2001:3::/64 [0/0]
  via ::, 00:32:59, vlan2
L 2001:3::1/128 [0/0]
  via ::, 00:32:58, vlan2
C 2001:4::/64 [0/0]
  via ::, 00:32:44, vlan3
L 2001:4::1/128 [0/0]
  via ::, 00:32:43, vlan3

```

According to the result, both Device2 and Device3 have learned the route of peer loopback interface by running OSPFv3 protocol. On this basis, Device2 and Device3 can establish IBGP neighbors through loopback interface.

Step 3: Configure basic functions of IPv6 BGP.

#Configure Device1.

Establish a direct EBGP peer with Device2, and import 2001:1::/64 into BGP through the network.

```

Device1#configure terminal
Device1(config)#router bgp 200
Device1(config-bgp)#bgp router-id 1.1.1.1
Device1(config-bgp)#address-family ipv6
Device1(config-bgp-af)#neighbor 2001:2::2 remote-as 100
Device1(config-bgp-af)#network 2001:1::/64
Device1(config-bgp-af)#exit-address-family
Device1(config-bgp)#exit

```

#Configure Device2.

Establish a direct EBGP peer with Device1, build indirect IBGP peer relationship with Device3 through Loopback0, and set the next hop of the advertised route as itself.

```

Device2(config)#router bgp 100
Device2(config-bgp)#bgp router-id 2.2.2.2
Device2(config-bgp)#address-family ipv6
Device2(config-bgp-af)#neighbor 2001:2::1 remote-as 200
Device2(config-bgp-af)#neighbor 2::2 remote-as 100
Device2(config-bgp-af)#neighbor 2::2 next-hop-self
Device2(config-bgp-af)#exit-address-family
Device2(config-bgp)#neighbor 2::2 update-source loopback 0
Device2(config-bgp)#exit

```

#Configure Device3.

Build indirect IBGP peer relationship with Device2 through Loopback0, and import 2001:4::/64 into BGP through the network.

```

Device3(config)#router bgp 100
Device3(config-bgp)#bgp router-id 3.3.3.3
Device3(config-bgp)#address-family ipv6
Device3(config-bgp-af)#neighbor 1::1 remote-as 100
Device3(config-bgp-af)#network 2001:4::/64
Device3(config-bgp-af)#exit-address-family
Device3(config-bgp)#neighbor 1::1 update-source loopback 0
Device3(config-bgp)#exit

```

---

 **Note**

- In order to avoid route flapping, IBGP neighbors are established through loopback interfaces. OSPFv3 is required to synchronize the routing information of the loopback interfaces between IBGP neighbors.
- 

Step 4: Check the result.

#View the status of IPv6 BGP neighbors on Device 2.

```
Device2#show bgp ipv6 unicast summary
BGP router identifier 2.2.2.2, local AS number 100
BGP table version is 4
2 BGP AS-PATH entries
0 BGP community entries

Neighbor    V  AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State/PfxRcd
2::2       4 100   8    6    3    0  00:04:12    1
2001:2::1  4 200  15   15    3    0  00:11:17    1

Total number of neighbors 2
```

From the case where the content of the State/PfxRcd column is displayed as a digit (from the number of routing prefixes received by the neighbor), you can see that Device 2 has successfully established IPv6 BGP neighbors with Device1 and Device3.

#View the routing table of Device1.

```
Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
  via ::, 1w2d:00:42:57, lo0
C 2001:1::/64 [0/0]
  via ::, 00:02:59, vlan2
L 2001:1::1/128 [0/0]
  via ::, 00:02:56, vlan2
C 2001:2::/64 [0/0]
  via ::, 00:52:17, vlan3
L 2001:2::1/128 [0/0]
  via ::, 00:52:16, vlan3
B 2001:4::/64 [20/0]
  via 2001:2::2, 00:06:13, vlan3
```

#View the routing table of Device 2.

```
Device2#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
  via ::, 1w2d:00:34:53, lo0
LC 1::1/128 [0/0]
  via ::, 00:52:49, loopback0
O 2::2/128 [110/2]
  via fe80::201:7aff:fec0:525a, 00:48:45, vlan2
```

```

B 2001:1::/64 [20/0]
  via 2001:2::1, 00:03:18, vlan3
C 2001:2::/64 [0/0]
  via ::, 00:52:57, vlan3
L 2001:2::2/128 [0/0]
  via ::, 00:52:55, vlan3
C 2001:3::/64 [0/0]
  via ::, 00:52:10, vlan2
L 2001:3::2/128 [0/0]
  via ::, 00:52:09, lo0
B 2001:4::/64 [200/0]
  via 2::2, 00:07:27, vlan2

```

#Check the routing table of Device3.

```

Device3#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

```

```

L ::1/128 [0/0]
  via ::, 1w5d:18:54:38, lo0
O 1::1/128 [110/2]
  via fe80::201:7aff:fe5e:6d2e, 00:49:44, vlan2
LC 2::2/128 [0/0]
  via ::, 00:52:21, loopback0
B 2001:1::/64 [200/0]
  via 1::1, 00:03:54, vlan2
C 2001:3::/64 [0/0]
  via ::, 00:52:44, vlan2
L 2001:3::1/128 [0/0]
  via ::, 00:52:43, vlan2
C 2001:4::/64 [0/0]
  via ::, 00:52:29, vlan3
L 2001:4::1/128 [0/0]
  via ::, 00:52:28, vlan3

```

According to the result, Device1 learns the direct route 2001:4::/64 from the interface of Device3 which learns the direct route 2001:1::/64 from the interface of Device1.

### 61.3.2 Configure IPv6 BGP route redistribution

#### Network Requirements

- Device3 establishes OSPFv3 neighbors with Device2, and advertises the direct route of the interface 2001:3::/64 to Device2.
- Establish EBGP neighbors between Device1 and Device2 so that Device2 will redistribute the OSPFv3 route to IPv6 BGP and advertise it to Device1.

#### Network Topology

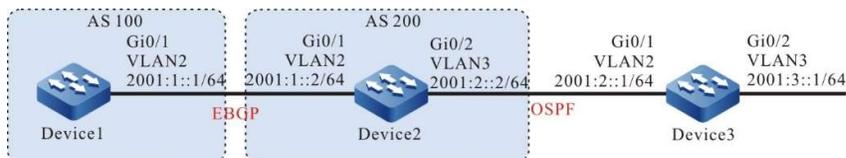


Figure 61 Network Topology for Configuring IPv6 BGP Route Redistribution

#### Configuration Steps

Step 1: Configure IPv6 global unicast address for interface. (Omitted)

Step 2: Configure OSPFv3 so that Device2 can learn the direct route 2001:3::/64 from Device3.

#### #Configure Device2.

```
Device2#configure terminal
Device2(config)#ipv6 router ospf 100
Device2(config-ospf6)#router-id 2.2.2.2
Device2(config-ospf6)#exit
Device2(config)#interface vlan 3
Device2(config-if-vlan3)#ipv6 router ospf 100 area 0
Device2(config-if-vlan3)#exit
```

#### #Configure Device3.

```
Device3#configure terminal
Device3(config)#ipv6 router ospf 100
Device3(config-ospf6)#router-id 3.3.3.3
Device3(config-ospf6)#exit
Device3(config)#interface vlan 2
Device3(config-if-vlan2)#ipv6 router ospf 100 area 0
Device3(config-if-vlan2)#exit
Device3(config)#interface vlan 3
Device3(config-if-vlan3)#ipv6 router ospf 100 area 0
Device3(config-if-vlan3)#exit
```

#### #View the routing table of Device 2.

```
Device2#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
  via ::, 1w2d:01:10:38, lo0
C 2001:1::/64 [0/0]
  via ::, 00:06:25, vlan2
L 2001:1::2/128 [0/0]
  via ::, 00:06:24, vlan2
C 2001:2::/64 [0/0]
  via ::, 00:05:46, vlan3
L 2001:2::2/128 [0/0]
  via ::, 00:05:43, vlan3
O 2001:3::/64 [110/2]
  via fe80::201:7aff:fec0:525a, 00:02:41, vlan3
```

It can be seen from the routing table that Device2 learns the OSPFv3 route 2001:3::/64 advertised by Device3.

Step 3: Configure basic functions of IPv6 BGP.

#### #Configure Device1.

```
Device1#configure terminal
Device1(config)#router bgp 100
Device1(config-bgp)#bgp router-id 1.1.1.1
Device1(config-bgp)#address-family ipv6
Device1(config-bgp-af)#neighbor 2001:1::2 remote-as 200
Device1(config-bgp-af)#exit-address-family
Device1(config-bgp)#exit
```

#### #Configure Device2.

```

Device2(config)#router bgp 200
Device2(config-bgp)#bgp router-id 2.2.2.2
Device2(config-bgp)#address-family ipv6
Device2(config-bgp-af)#neighbor 2001::1 remote-as 100
Device2(config-bgp-af)#exit-address-family
Device2(config-bgp)#exit

```

#View the status of IPv6 BGP neighbors on Device 2.

```

Device2#show bgp ipv6 unicast summary
BGP router identifier 2.2.2.2, local AS number 200
BGP table version is 1
1 BGP AS-PATH entries
0 BGP community entries

Neighbor      V  AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State/PfxRcd
2001::1:1    4 100    2    2    1    0 00:00:50    0

Total number of neighbors 1

```

#According to the result, IPv6 BGP neighbors have been successfully established between Device 2 and Device1.

Step 4: Configure IPv6 BGP to redistribute OSPFv3 route.

#Configure Device2.

```

Device2(config)#router bgp 200
Device2(config-bgp)#address-family ipv6
Device2(config-bgp-af)#redistribute ospf 100
Device2(config-bgp-af)#exit-address-family
Device2(config-bgp)#exit

```

Step 5: Check the result.

#View the IPv6 BGP routing table of Device2.

```

Device2#show bgp ipv6 unicast
BGP table version is 2, local router ID is 2.2.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Network      Next Hop      Metric  LocPrf Weight Path
[O]*> 2001:2::/64  ::           1      32768 ?
[O]*> 2001:3::/64  ::           2      32768 ?

```

According to the result, OSPFv3 route has been successfully redistributed to IPv6 BGP.

#View the routing table of Device1.

```

Device1#show bgp ipv6 unicast
BGP table version is 3, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Network      Next Hop      Metric  LocPrf Weight Path
[B]*> 2001:2::/64  2001:1::2    1        0 200 ?
[B]*> 2001:3::/64  2001:1::2    2        0 200 ?

```

According to the result, Device1 has successfully learnt the routes 2001:2::/64 and 2001:3::/64.



说明：

- In practical applications, if the autonomous system has 2 or more edge devices, directly redistributing routes between different routing protocols is not recommended. When configuration is necessary, routing control policies such as filtering and summarization are required on the edge devices of the autonomous system to avoid routing loops.

### 61.3.3 Configure IPv6 BGP community attributes

#### Network Requirements

- EBMP neighbors are successfully established between Device1 and Device2.
- Device1 imports two direct routes 2001:1::/64 and 2001:2::/64 into BGP through the network, and sets different community attributes for the two routes when they are advertised to Device2.
- When Device2 receives the route advertised by Device1, it filters the route 2001:1::/64 in the incoming direction of the neighbor by matching community attributes, and permits the route 2001:2::/64 to pass.

#### Network Topology

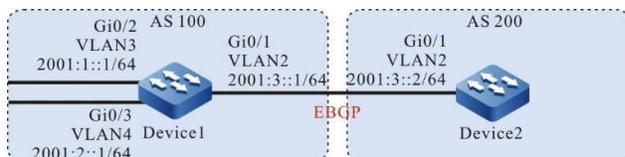


Figure 1 Network Topology for Configuring Community Attributes of IPv6 BGP

#### Configuration Steps

Step 1: Configure IPv6 global unicast address for interface. (Omitted)

Step 2: Configure basic functions of IPv6 BGP.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#router bgp 100
Device1(config-bgp)#bgp router-id 1.1.1.1
Device1(config-bgp)#address-family ipv6
Device1(config-bgp-af)#neighbor 2001:3::2 remote-as 200
Device1(config-bgp-af)#network 2001:1::/64
Device1(config-bgp-af)#network 2001:2::/64
Device1(config-bgp-af)#exit-address-family
Device1(config-bgp)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#router bgp 200
```

```

Device2(config-bgp)#bgp router-id 2.2.2.2
Device2(config-bgp)#address-family ipv6
Device2(config-bgp-af)#neighbor 2001:3::1 remote-as 100
Device2(config-bgp-af)#exit-address-family
Device2(config-bgp)#exit

```

#View the status of IPv6 BGP neighbors on Device1.

```

Device1#show bgp ipv6 unicast summary
BGP router identifier 1.1.1.1, local AS number 100
BGP table version is 1
1 BGP AS-PATH entries
0 BGP community entries

Neighbor    V  AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State/PfxRcd
2001:3::2   4  200    3    4    1    0  00:01:02    0

Total number of neighbors 1

```

#It can be seen that IPv6 BGP neighbors have been successfully established between Device 1 and Device2.

#View the routing table on Device2.

```

Device2#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L  ::1/128 [0/0]
   via ::, Iw2d:05:45:34, lo0
B  2001:1::/64 [20/0]
   via 2001:3::1, 00:01:35, vlan2
B  2001:2::/64 [20/0]
   via 2001:3::1, 00:01:35, vlan2
C  2001:3::/64 [0/0]
   via ::, 00:04:09, vlan2
L  2001:3::2/128 [0/0]
   via ::, 00:04:08, vlan2

```

According to the result, Device2 has successfully learnt the routes 2001:1::/64 and 2001:2::/64.

Step 3: Configure access list and routing policy, and set IPv6 BGP community attributes.

#Configure Device1.

```

Device1(config)#ipv6 access-list extended 7001
Device1(config-v6-list)#permit ipv6 2001:1::/64 any
Device1(config-v6-list)#commit
Device1(config-v6-list)#exit
Device1(config)#ipv6 access-list extended 7002
Device1(config-v6-list)#permit ipv6 2001:2::/64 any
Device1(config-v6-list)#commit
Device1(config-v6-list)#exit
Device1(config)#route-map CommunitySet 10
Device1(config-route-map)#match ipv6 address 7001
Device1(config-route-map)#set community 100:1
Device1(config-route-map)#exit
Device1(config)#route-map CommunitySet 20
Device1(config-route-map)#match ipv6 address 7002
Device1(config-route-map)#set community 100:2
Device1(config-route-map)#exit

```

Set different community attributes for the routes 2001:1::/64 and 2001:2::/64 by configuring access list and routing policy.

Step 4: Configure IPv6 BGP to associate routing policy.

#Configure Device1.

```
Device1(config)#router bgp 100
Device1(config-bgp)#address-family ipv6
Device1(config-bgp-af)#neighbor 2001:3::2 route-map CommunitySet out
Device1(config-bgp-af)#neighbor 2001:3::2 send-community
Device1(config-bgp-af)#exit-address-family
Device1(config-bgp)#exit
```

#View the IPv6 BGP routing table of Device2.

```
Device2#show bgp ipv6 unicast 2001:1::/64
BGP routing table entry for 2001:1::/64
Paths: (1 available, best #1, table Default-IP-Routing-Table)
Not advertised to any peer
100
2001:3::1 (metric 10) from 2001:3::1 (1.1.1.1)

Origin IGP, metric 0, localpref 100, valid, external, best
Community: 100:1
Last update: 00:00:24 ago
Device2#show bgp ipv6 unicast 2001:2::/64
BGP routing table entry for 2001:2::/64
Paths: (1 available, best #1, table Default-IP-Routing-Table)
Not advertised to any peer
100
2001:3::1 (metric 10) from 2001:3::1 (1.1.1.1)

Origin IGP, metric 0, localpref 100, valid, external, best
Community: 100:2
Last update: 00:00:30 ago
```

It can be seen from the IPv6 BGP routing table of Device2 that the community attribute of 2001:1::/64 has been set as 100:1, and that of 2001:2::/64 as 100:2.

Step 5: Configure IPv6 BGP route filtration.

#Configure Device2.

```
Device2(config)#ip community-list 1 permit 100:2
Device2(config)#route-map CommunityFilter
Device2(config-route-map)#match community 1
Device2(config-route-map)#exit
Device2(config)#router bgp 200
Device2(config-bgp)#address-family ipv6
Device2(config-bgp-af)#neighbor 2001:3::1 route-map CommunityFilter in
Device2(config-bgp-af)#exit-address-family
Device2(config-bgp)#exit
```

Step 6: Check the result.

#View the routing table of Device 2.

```
Device2#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
U - Per-user Static route
O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
via ::, 1w2d:05:58:57, lo0
```

```

B 2001:2::/64 [20/0]
  via 2001:3::1, 00:00:05, vlan2
C 2001:3::/64 [0/0]
  via ::, 00:17:32, vlan2
L 2001:3::2/128 [0/0]
  via ::, 00:17:30, vlan2

```

It can be seen from the IPv6 BGP routing table of Device2 that 2001:1::/64 is filtered in the incoming direction, while 2001:2::/64 is allowed to pass.

## Note

- After configuring the routing policy on IPv6 BGP neighbors, it is required to reset the IPv6 BGP neighbors to make it take effect.
- The command **send-community** is required to advertise the community attributes to the peer.

### 61.3.4 Configure IPv6 BGP route reflector

#### Network Requirements

- Device3 establishes EBGP neighbors with Device4 which advertises the route of the 2001:4::/64 to Device3.
- Device2 establishes IBGP neighbors with Device3 and Device1 respectively. Route reflector is configured on Device2. Device1 and Device3 serve as clients so that Device1 can learn the route 2001:4::/64 advertised by Device4.

#### Network Topology

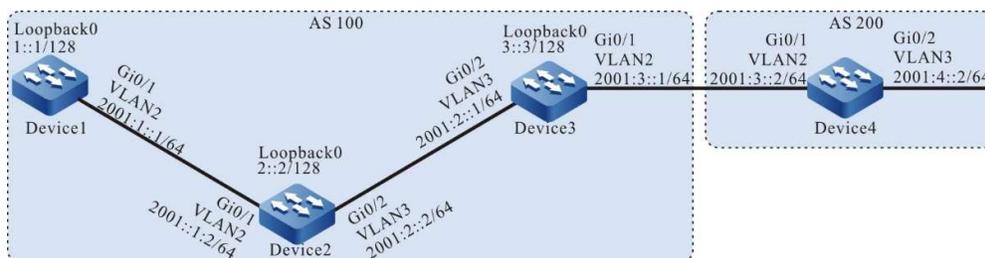


Figure 61 Network Topology for Configuring IPv6 BGP Route Reflector

#### Configuration Steps

- Step 1: Configure IPv6 global unicast address for interface. (Omitted)
- Step 2: Configure OSPFv3 so that the routes of Loopback interfaces between devices are reachable from each other.

#Configure Device1.

```

Device1#configure terminal
Device1(config)#ipv6 router ospf 100
Device1(config-ospf6)#router-id 1.1.1.1
Device1(config-ospf6)#exit
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#ipv6 router ospf 100 area 0
Device1(config-if-vlan2)#exit
Device1(config)#interface loopback 0
Device1(config-if-loopback0)#ipv6 router ospf 100 area 0
Device1(config-if-loopback0)#exit

```

### #Configure Device2.

```

Device2#configure terminal
Device2(config)#ipv6 router ospf 100
Device2(config-ospf6)#router-id 2.2.2.2
Device2(config-ospf6)#exit
Device2(config)#interface vlan 2
Device2(config-if-vlan2)#ipv6 router ospf 100 area 0
Device2(config-if-vlan2)#exit
Device2(config)#interface vlan 3
Device2(config-if-vlan3)#ipv6 router ospf 100 area 0
Device2(config-if-vlan3)#exit
Device2(config)#interface loopback 0
Device2(config-if-loopback0)#ipv6 router ospf 100 area 0
Device2(config-if-loopback0)#exit

```

### #Configure Device3.

```

Device3#configure terminal
Device3(config)#ipv6 router ospf 100
Device3(config-ospf6)#router-id 3.3.3.3
Device3(config-ospf6)#exit
Device3(config)#interface vlan 3
Device3(config-if-vlan3)#ipv6 router ospf 100 area 0
Device3(config-if-vlan3)#exit
Device3(config)#interface loopback 0
Device3(config-if-loopback0)#ipv6 router ospf 100 area 0
Device3(config-if-loopback0)#exit

```

### #View the routing table of Device1.

```

Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L  ::1/128 [0/0]
   via ::, 1w2d:06:26:16, lo0
LC 1::1/128 [0/0]
   via ::, 00:13:56, loopback0
O  2::2/128 [110/2]
   via fe80::201:7aff:fec0:525a, 00:09:06, vlan2
O  3::3/128 [110/3]
   via fe80::201:7aff:fec0:525a, 00:00:36, vlan2
C  2001:1::/64 [0/0]
   via ::, 00:14:03, vlan2
L  2001:1::1/128 [0/0]
   via ::, 00:14:02, vlan2
O  2001:2::/64 [110/2]
   via fe80::201:7aff:fec0:525a, 00:09:06, vlan2

```

### #View the routing table of Device 2.

```

Device2#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

```

```

L ::1/128 [0/0]
  via ::, 1w6d:00:46:09, lo0
O 1::1/128 [110/2]
  via fe80::201:7aff:fe5e:6d2e, 00:10:05, vlan2
LC 2::2/128 [0/0]
  via ::, 00:14:23, loopback0
O 3::3/128 [110/2]
  via fe80::201:7aff:fe62:bb80, 00:01:44, vlan3
C 2001:1::/64 [0/0]
  via ::, 00:14:48, vlan2
L 2001:1::2/128 [0/0]
  via ::, 00:14:47, vlan2
C 2001:2::/64 [0/0]
  via ::, 00:14:41, vlan3
L 2001:2::2/128 [0/0]
  via ::, 00:14:39, vlan3

```

#Check the routing table of Device3.

```

Device3#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

```

```

L ::1/128 [0/0]
  via ::, 1w2d:06:37:24, lo0
O 1::1/128 [110/3]
  via fe80::201:7aff:fec0:525b, 00:02:39, vlan3
O 2::2/128 [110/2]
  via fe80::201:7aff:fec0:525b, 00:02:39, vlan3
LC 3::3/128 [0/0]
  via ::, 00:14:45, loopback0
O 2001:1::/64 [110/2]
  via fe80::201:7aff:fec0:525b, 00:02:39, vlan3
C 2001:2::/64 [0/0]
  via ::, 00:15:03, vlan3
L 2001:2::1/128 [0/0]
  via ::, 00:15:02, vlan3
C 2001:3::/64 [0/0]
  via ::, 00:14:55, vlan2
L 2001:3::1/128 [0/0]
  via ::, 00:14:54, vlan2

```

It can be seen that Device1, Device2 and Device3 can learn the routes of their loopback interface from each other.

Step 3: Configure basic functions of IPv6 BGP.

#Configure Device1.

```

Device1(config)#router bgp 100
Device1(config-bgp)#bgp router-id 1.1.1.1
Device1(config-bgp)#address-family ipv6
Device1(config-bgp-af)#neighbor 2::2 remote-as 100
Device1(config-bgp-af)#exit-address-family
Device1(config-bgp)#neighbor 2::2 update-source loopback 0
Device1(config-bgp)#exit

```

#Configure Device2.

```

Device2(config)#router bgp 100
Device2(config-bgp)#bgp router-id 2.2.2.2
Device2(config-bgp)#address-family ipv6
Device2(config-bgp-af)#neighbor 1::1 remote-as 100
Device2(config-bgp-af)#neighbor 3::3 remote-as 100
Device2(config-bgp-af)#exit-address-family
Device2(config-bgp)#neighbor 1::1 update-source loopback 0

```

```
Device2(config-bgp)#neighbor 3::3 update-source loopback 0
Device2(config-bgp)#exit
```

### #Configure Device3.

```
Device3(config)#router bgp 100
Device3(config-bgp)#bgp router-id 3.3.3.3
Device3(config-bgp)#address-family ipv6
Device3(config-bgp-af)#neighbor 2::2 remote-as 100
Device3(config-bgp-af)#neighbor 2::2 next-hop-self
Device3(config-bgp-af)#neighbor 2001:3::2 remote-as 200
Device3(config-bgp-af)#exit-address-family
Device3(config-bgp)#neighbor 2::2 update-source loopback 0
Device3(config-bgp)#exit
```

### #Configure Device4.

```
Device4#configure terminal
Device4(config)#router bgp 200
Device4(config-bgp)#bgp router-id 4.4.4.4
Device4(config-bgp)#address-family ipv6
Device4(config-bgp-af)#neighbor 2001:3::1 remote-as 100
Device4(config-bgp-af)#network 2001:4::/64
Device4(config-bgp-af)#exit-address-family
Device4(config-bgp)#exit
```

### #View the status of IPv6 BGP neighbors on Device 2.

```
Device2#show bgp ipv6 unicast summary
BGP router identifier 2.2.2.2, local AS number 100
BGP table version is 2
2 BGP AS-PATH entries
0 BGP community entries

Neighbor    V  AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State/PfxRcd
1::1        4  100   10   10     2  0  0 00:07:18    0
3::3        4  100   10    9     2  0  0 00:06:53    1

Total number of neighbors 2
```

### #View the status of IPv6 BGP neighbors on Device4.

```
Device4#show bgp ipv6 unicast summary
BGP router identifier 4.4.4.4, local AS number 200
BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries

Neighbor    V  AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State/PfxRcd
2001:3::1   4  100    3    4     2  0  0 00:01:45    0

Total number of neighbors 1
```

It can be seen that IPv6 BGP neighbors have been successfully established between devices.

### #View the IPv6 BGP routing table of Device3.

```
Device3#show bgp ipv6 unicast
BGP table version is 3, local router ID is 3.3.3.3
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Network      Next Hop      Metric  LocPrf Weight Path
[B]*> 2001:4::/64  2001:3::2      0         0 200 i
```

### #View the IPv6 BGP routing table of Device2.

```
Device2#show bgp ipv6 unicast
BGP table version is 7, local router ID is 2.2.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
```

```

S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Network      Next Hop      Metric  LocPrf Weight Path
[B]*>i2001:4::/64    3::3          0      100   0 200 i

```

#View the IPv6 BGP routing table of Device1.

```
Device1#show bgp ipv6 unicast
```

It can be seen from above that both Device2 and Device3 have learned the route 2001:4::/64, though Device2 doesn't advertise it to Device1.

Step 4: Configure IPv6 BGP route reflector.

#Configure Device2.

```

Device2(config)#router bgp 100
Device2(config-bgp)#address-family ipv6
Device2(config-bgp-af)#neighbor 1::1 route-reflector-client
Device2(config-bgp-af)#neighbor 3::3 route-reflector-client
Device2(config-bgp-af)#exit-address-family
Device2(config-bgp)#exit

```

On Device2, configure Device1 and Device3 as clients of route reflector.

Step 5: Check the result.

#View the routing table of Device1.

```

Device1#show bgp ipv6 unicast
BGP table version is 2, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Network      Next Hop      Metric  LocPrf Weight Path
[B]*>i2001:4::/64    3::3          0      100   0 200 i
Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
U - Per-user Static route
O - OSPF, OE-OSPF External, M - Management

```

```

L ::1/128 [0/0]
via ::, 1w2d:06:48:52, lo0
LC 1::1/128 [0/0]
via ::, 00:36:32, loopback0
O 2::2/128 [110/2]
via fe80::201:7aff:fec0:525a, 00:31:42, vlan2
O 3::3/128 [110/3]
via fe80::201:7aff:fec0:525a, 00:23:12, vlan2
C 2001:1::/64 [0/0]
via ::, 00:36:39, vlan2
L 2001:1::1/128 [0/0]
via ::, 00:36:38, vlan2
O 2001:2::/64 [110/2]
via fe80::201:7aff:fec0:525a, 00:31:42, vlan2
B 2001:4::/64 [200/0]
via 3::3, 00:01:16, vlan2

```

Configure Device1 and Device3 as clients of route reflector in the BGP of Device2 which successfully reflects the route 2001:4::/64 to the client Device1.

---

## Note

- When a IPv6 BGP neighbor is configured as the client of route reflector, this neighbor will be reset.
- 

### 61.3.5 Configure IPv6 BGP route aggregation

#### Network Requirements

- Device1 establishes OSPFv3 neighbors with Device3 which advertises the two routes 2002:1::/64 and 2002:2::/64 to Device1.
- EBMP neighbors are successfully established between Device1 and Device2.
- On Device1, the routes 2002:1::/64 and 2002:2::/64 are aggregated into 2002::/30 to advertise to Device2.

#### Network Topology

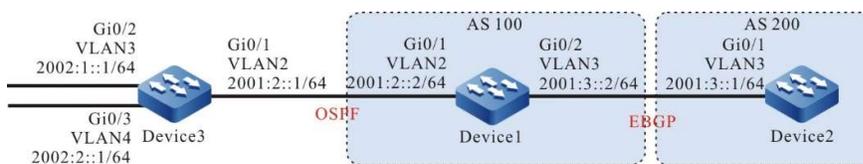


Figure 61 Network Topology for Configuring IPv6 BGP Route Aggregation

#### Configuration Steps

- Step 1: Configure IPv6 global unicast address for interface. (Omitted)
- Step 2: Configure OSPFv3 so that Device1 can learn the two routes 2002:1::/64 and 2002:2::/64 advertised by Device3.

#### #Configure Device1.

```
Device1#configure terminal
Device1(config)#ipv6 router ospf 100
Device1(config-ospf6)#router-id 1.1.1.1
Device1(config-ospf6)#exit
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#ipv6 router ospf 100 area 0
Device1(config-if-vlan2)#exit
```

#### #Configure Device3.

```
Device3#configure terminal
Device3(config)#ipv6 router ospf 100
Device3(config-ospf6)#router-id 3.3.3.3
Device3(config-ospf6)#exit
Device3(config)#interface vlan 2
Device3(config-if-vlan2)#ipv6 router ospf 100 area 0
Device3(config-if-vlan2)#exit
Device3(config)#interface vlan 3
```

```

Device3(config-if-vlan3)#ipv6 router ospf 100 area 0
Device3(config-if-vlan3)#exit
Device3(config)#interface vlan 4
Device3(config-if-vlan4)#ipv6 router ospf 100 area 0
Device3(config-if-vlan4)#exit

```

### #View the routing table of Device1.

```

Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
  via ::, 1w2d:07:35:38, lo0
C 2001:3::/64 [0/0]
  via ::, 00:01:11, vlan3
L 2001:3::2/128 [0/0]
  via ::, 00:01:10, vlan3
C 2001:2::/64 [0/0]
  via ::, 00:01:06, vlan2
L 2001:2::2/128 [0/0]
  via ::, 00:01:04, vlan2
O 2002:1::/64 [110/2]
  via fe80::201:7aff:fe62:bb7e, 00:01:54, vlan2
O 2002:2::/64 [110/2]
  via fe80::201:7aff:fe62:bb7e, 00:01:54, vlan2

```

It can be seen that Device1 learns the two routes 2002:1:1::/64 and 2002:1:2::/64 distributed by Device3.

### Step 3: Configure basic functions of IPv6 BGP.

#### #Configure Device1.

```

Device1(config)#router bgp 100
Device1(config-bgp)#bgp router-id 1.1.1.1
Device1(config-bgp)#address-family ipv6
Device1(config-bgp-af)#neighbor 2001:3::1 remote-as 200
Device1(config-bgp-af)#exit-address-family
Device1(config-bgp)#exit

```

#### #Configure Device2.

Device2#configure terminal

```

Device2(config)#router bgp 200
Device2(config-bgp)#bgp router-id 2.2.2.2
Device2(config-bgp)#address-family ipv6
Device2(config-bgp-af)#neighbor 2001:3::2 remote-as 100
Device2(config-bgp-af)#exit-address-family
Device2(config-bgp)#exit

```

#### #View the status of IPv6 BGP neighbors on Device1.

```

Device1#show bgp ipv6 unicast summary
BGP router identifier 1.1.1.1, local AS number 100
BGP table version is 1
1 BGP AS-PATH entries
0 BGP community entries

Neighbor    V  AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State/PfxRcd
2001:3::1   4  200   3    3    1    0  00:01:16    0

```

IPv6 BGP neighbors have been successfully established between Device 1 and Device2.

Step 4: Configure IPv6 BGP route aggregation.

To meet the network requirements, here are two schemes:

Scheme 1: Configure IPv6 static route pointing to null0 and import it into BGP.

#Configure Device1.

```
Device1(config)#ipv6 route 2002::/30 null 0
Device1(config)#router bgp 100
Device1(config-bgp)#address-family ipv6
Device1(config-bgp-af)#network 2002::/30
Device1(config-bgp-af)#exit-address-family
Device1(config-bgp)#exit
```

Check the result.

#View the IPv6 BGP routing table of Device1.

```
Device1#show bgp ipv6 unicast
BGP table version is 2, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop        Metric   LocPrf Weight Path
[B]*> 2002::/30   ::              0        32768 i
```

It can be seen that the aggregated route 2002::/30 has been generated in the IPv6 BGP routing table of Device1.

#View the routing table of Device 2.

```
Device2#show bgp ipv6 unicast
BGP table version is 2, local router ID is 2.2.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop        Metric   LocPrf Weight Path
[B]*> 2002::/30   2001:3::2       0         0 100 i
Device2#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
  via ::, 1w6d:03:14:01, lo0
C 2001:3::/64 [0/0]
  via ::, 01:20:21, vlan3
L 2001:3::1/128 [0/0]
  via ::, 01:20:20, vlan3
B 2002::/30 [20/0]
  via 2001:3::2, 00:00:44, vlan3
```

It can be seen that Device2 has successfully learned the aggregated route 2002::/30 advertised by Device1.

Scheme 2: First import the detail route into BGP and then complete route aggregation via the command aggregate-address.

#Configure Device1.

```
Device1(config)#router bgp 100
Device1(config-bgp)#address-family ipv6
Device1(config-bgp-af)#redistribute ospf 100
```

```

Device1(config-bgp-af)#aggregate-address 2002::/30 summary-only
Device1(config-bgp-af)#exit-address-family
Device1(config-bgp)#exit

```

Check the result.

#### #View the IPv6 BGP routing table of Device1.

```

Device1#show bgp ipv6 unicast
BGP table version is 4, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop        Metric    LocPrf Weight Path
[O]*> 2001:2::/64  ::              1         32768 ?
[B]*> 2002::/30   ::              32768 i
[O]s> 2002:1::/64  ::              2         32768 ?
[O]s> 2002:2::/64  ::              2         32768 ?

```

It can be seen that the aggregated route 2002::/30 has been generated in the IPv6 BGP routing table of Device1.

#### #View the routing table of Device 2.

```

Device2#show bgp ipv6 unicast
BGP table version is 4, local router ID is 2.2.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop        Metric    LocPrf Weight Path
[B]*> 2001:2::/64  2001:3::2      1         0 100 ?
[B]*> 2002::/30   2001:3::2      0         0 100 i
Device2#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

```

```

L ::1/128 [0/0]
  via ::, 1w6d:03:16:42, lo0
B 2001:2::/64 [20/0]
  via 2001:3::2, 00:00:50, vlan3
C 2001:3::/64 [0/0]
  via ::, 01:23:01, vlan3
L 2001:3::1/128 [0/0]
  via ::, 01:23:00, vlan3
B 2002::/30 [20/0]
  via 2001:3::2, 00:00:50, vlan3

```

It can be seen that Device2 has successfully learned the aggregated route 2002::/30 advertised by Device1.

---

### Note

- When the command `aggregate-address` is used for route aggregation, if the extension command `summary-only` is configured, the device will advertise aggregated route only; otherwise, it will advertise both detail route and aggregated route.
-

## 61.3.6 Configure IPv6 BGP route preference

### Network Requirements

- Device1 has established IBGP neighbors with Device2 and Device3, and Device4 has established EBGP neighbors with Device2 and Device3.
- Device1 advertises two routes to Device4, i.e. 2001:1::/64 and 2001:2::/64; Device4 advertises two routes to Device1, i.e. 2001:7::/64 and 2001:8::/64.
- By modifying the Local-preference of route on Device2 and Device3, you can make Device1 prefer the route 2001:7::/64 advertised by Device3 and the route 2001:8::/64 advertised by Device2.
- By modifying the MED of route on Device2 and Device3, you can make Device4 prefer the route 2001:1::/64 advertised by Device3 and the route 2001:2::/64 advertised by Device2.

### Network Topology

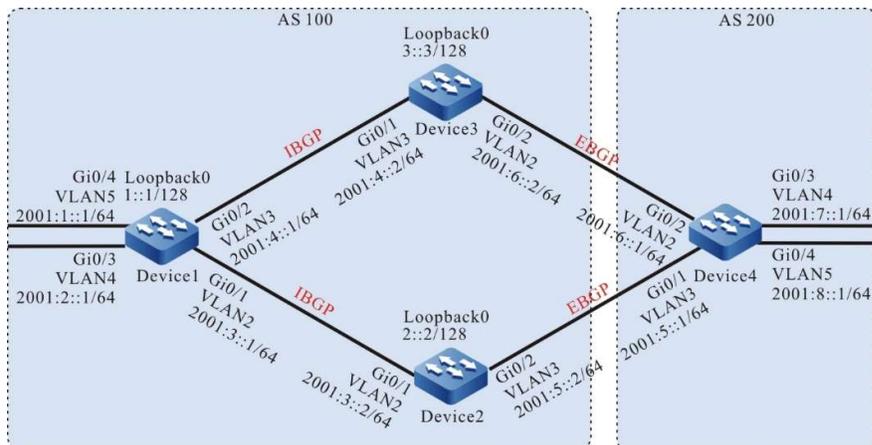


Figure 61 Network Topology for Configuring IPv6 BGP Route Preference

### Configuration Steps

- Step 1: Configure IPv6 global unicast address for interface. (Omitted)
- Step 2: Configure OSPFv3 so that the routes of Loopback interfaces between devices are reachable from each other.

#### #Configure Device1.

```
Device1#configure terminal
Device1(config)#ipv6 router ospf 100
Device1(config-ospf6)#router-id 1.1.1.1
Device1(config-ospf6)#exit
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#ipv6 router ospf 100 area 0
```

```

Device1(config-if-vlan2)#exit
Device1(config)#interface vlan 3
Device1(config-if-vlan3)#ipv6 router ospf 100 area 0
Device1(config-if-vlan3)#exit
Device1(config)#interface loopback 0
Device1(config-if-loopback0)#ipv6 router ospf 100 area 0
Device1(config-if-loopback0)#exit

```

### #Configure Device2.

```

Device2#configure terminal
Device2(config)#ipv6 router ospf 100
Device2(config-ospf6)#router-id 2.2.2.2
Device2(config-ospf6)#exit
Device2(config)#interface vlan 2
Device2(config-if-vlan2)#ipv6 router ospf 100 area 0
Device2(config-if-vlan2)#exit
Device2(config)#interface loopback 0
Device2(config-if-loopback0)#ipv6 router ospf 100 area 0
Device2(config-if-loopback0)#exit

```

### #Configure Device3.

```

Device3#configure terminal
Device3(config)#ipv6 router ospf 100
Device3(config-ospf6)#router-id 3.3.3.3
Device3(config-ospf6)#exit
Device3(config)#interface vlan 3
Device3(config-if-vlan3)#ipv6 router ospf 100 area 0
Device3(config-if-vlan3)#exit
Device3(config)#interface loopback 0
Device3(config-if-loopback0)#ipv6 router ospf 100 area 0
Device3(config-if-loopback0)#exit

```

### #View the routing table of Device1.

```

Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
   via ::, 1w5d:04:03:11, lo0
LC 1::1/128 [0/0]
   via ::, 00:08:39, loopback0
O 2::2/128 [110/2]
   via fe80::201:7aff:fe5e:87da, 00:02:04, vlan2
O 3::3/128 [110/2]
   via fe80::201:7aff:fec0:525b, 00:00:38, vlan3
C 2001:1::/64 [0/0]
   via ::, 00:09:12, vlan5
L 2001:1::1/128 [0/0]
   via ::, 00:09:11, vlan5
C 2001:2::/64 [0/0]
   via ::, 00:08:26, vlan4
L 2001:2::1/128 [0/0]
   via ::, 00:08:26, vlan4
C 2001:3::/64 [0/0]
   via ::, 00:09:01, vlan2
L 2001:3::1/128 [0/0]
   via ::, 00:09:00, vlan2
C 2001:4::/64 [0/0]
   via ::, 00:08:55, vlan3
L 2001:4::1/128 [0/0]
   via ::, 00:08:53, vlan3

```

### #View the routing table of Device 2.

```

Device2#show ipv6 route

```

Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS  
U - Per-user Static route  
O - OSPF, OE-OSPF External, M - Management

```
L ::1/128 [0/0]
  via ::, 2w4d:23:16:51, lo0
O 1::1/128 [110/2]
  via fe80::201:7aff:fe62:bb7f, 00:04:25, vlan2
LC 2::2/128 [0/0]
  via ::, 00:09:31, loopback0
O 3::3/128 [110/3]
  via fe80::201:7aff:fe62:bb7f, 00:02:52, vlan2
C 2001:3::/64 [0/0]
  via ::, 00:09:49, vlan2
L 2001:3::2/128 [0/0]
  via ::, 00:09:48, vlan2
O 2001:4::/64 [110/2]
  via fe80::201:7aff:fe62:bb7f, 00:04:25, vlan2
C 2001:5::/64 [0/0]
  via ::, 00:09:39, vlan3
L 2001:5::2/128 [0/0]
  via ::, 00:09:38, vlan3
```

### #Check the routing table of Device3.

```
Device3#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
U - Per-user Static route
O - OSPF, OE-OSPF External, M - Management
```

```
L ::1/128 [0/0]
  via ::, 2w1d:22:16:55, lo0
O 1::1/128 [110/2]
  via fe80::201:7aff:fe62:bb80, 00:04:27, vlan3
O 2::2/128 [110/3]
  via fe80::201:7aff:fe62:bb80, 00:04:27, vlan3
LC 3::3/128 [0/0]
  via ::, 00:10:48, loopback0
O 2001:3::/64 [110/2]
  via fe80::201:7aff:fe62:bb80, 00:04:27, vlan3
C 2001:4::/64 [0/0]
  via ::, 00:11:55, vlan3
L 2001:4::2/128 [0/0]
  via ::, 00:11:54, vlan3
C 2001:6::/64 [0/0]
  via ::, 00:11:48, vlan2
L 2001:6::2/128 [0/0]
  via ::, 00:11:47, vlan2
```

It can be seen that Device1, Device2 and Device3 can learn the routes of their loopback interface from each other.

### Step 3: Configure basic functions of IPv6 BGP.

#### #Configure Device1.

```
Device1(config)#router bgp 100
Device1(config-bgp)#bgp router-id 1.1.1.1
Device1(config-bgp)#address-family ipv6
Device1(config-bgp-af)#neighbor 2::2 remote-as 100
Device1(config-bgp-af)#neighbor 3::3 remote-as 100
Device1(config-bgp-af)#network 2001:1::/64
Device1(config-bgp-af)#network 2001:2::/64
Device1(config-bgp-af)#exit-address-family
Device1(config-bgp)#neighbor 2::2 update-source loopback 0
Device1(config-bgp)#neighbor 3::3 update-source loopback 0
```

```
Device1(config-bgp)#exit
```

#### #Configure Device2.

```
Device2(config)#router bgp 100
Device2(config-bgp)#bgp router-id 2.2.2.2
Device2(config-bgp)#address-family ipv6
Device2(config-bgp-af)#neighbor 1::1 remote-as 100
Device2(config-bgp-af)#neighbor 1::1 next-hop-self
Device2(config-bgp-af)#neighbor 2001:5::1 remote-as 200
Device2(config-bgp-af)#exit-address-family
Device2(config-bgp)#neighbor 1::1 update-source loopback 0
Device2(config-bgp)#exit
```

#### #Configure Device3.

```
Device3(config)#router bgp 100
Device3(config-bgp)#bgp router-id 3.3.3.3
Device3(config-bgp)#address-family ipv6
Device3(config-bgp-af)#neighbor 1::1 remote-as 100
Device3(config-bgp-af)#neighbor 1::1 next-hop-self
Device3(config-bgp-af)#neighbor 2001:6::1 remote-as 200
Device3(config-bgp-af)#exit-address-family
Device3(config-bgp)#neighbor 1::1 update-source loopback 0
Device3(config-bgp)#exit
```

#### #Configure Device4.

```
Device4#configure terminal
Device4(config)#router bgp 200
Device4(config-bgp)#bgp router-id 4.4.4.4
Device4(config-bgp)#address-family ipv6
Device4(config-bgp-af)#neighbor 2001:5::2 remote-as 100
Device4(config-bgp-af)#neighbor 2001:6::2 remote-as 100
Device4(config-bgp-af)#network 2001:7::/64
Device4(config-bgp-af)#network 2001:8::/64
Device4(config-bgp-af)#exit-address-family
Device4(config-bgp)#exit
```

#### #View the status of IPv6 BGP neighbors on Device1.

```
Device1#show bgp ipv6 unicast summary
BGP router identifier 1.1.1.1, local AS number 100
BGP table version is 4
2 BGP AS-PATH entries
0 BGP community entries

Neighbor    V  AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State/PfxRed
2::2       4 100    9   10    4   0  00:06:18    2
3::3       4 100    7    8    4   0  00:04:29    2

Total number of neighbors 2
```

#### #View the status of IPv6 BGP neighbors on Device4.

```
Device4#show bgp ipv6 unicast summary
BGP router identifier 4.4.4.4, local AS number 200
BGP table version is 4
2 BGP AS-PATH entries
0 BGP community entries

Neighbor    V  AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State/PfxRed
2001:5::2  4 100    6    5    4   0  00:02:43    2
2001:6::2  4 100    5    6    4   0  00:02:32    2

Total number of neighbors 2
```

According to the result, Device1 has successfully established IBGP neighbors with Device2 and Device3, and Device4 has successfully established EBGP neighbors with Device2 and Device3.

## #View the routing table of Device1.

```
Device1#show bgp ipv6 unicast
BGP table version is 4, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop        Metric   LocPrf Weight Path
[B]*> 2001:1::/64  ::              0        32768 i
[B]*> 2001:2::/64  ::              0        32768 i
[B]* i2001:7::/64  3::3           0        100   0 200 i
[B]*>i            2::2           0        100   0 200 i
[B]*>i2001:8::/64  2::2           0        100   0 200 i
[B]* i           3::3           0        100   0 200 i

Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management
```

```
L ::1/128 [0/0]
   via ::, 1w5d:04:20:19, lo0
LC 1::1/128 [0/0]
   via ::, 00:25:47, loopback0
O 2::2/128 [110/2]
   via fe80::201:7aff:fe5e:87da, 00:19:12, vlan2
O 3::3/128 [110/2]
   via fe80::201:7aff:fec0:525b, 00:17:46, vlan3
C 2001:1::/64 [0/0]
   via ::, 00:26:20, vlan5
L 2001:1::1/128 [0/0]
   via ::, 00:26:19, vlan5
C 2001:2::/64 [0/0]
   via ::, 00:25:34, vlan4
L 2001:2::1/128 [0/0]
   via ::, 00:25:34, vlan4
C 2001:3::/64 [0/0]
   via ::, 00:26:09, vlan2
L 2001:3::1/128 [0/0]
   via ::, 00:26:08, vlan2
C 2001:4::/64 [0/0]
   via ::, 00:26:03, vlan3
L 2001:4::1/128 [0/0]
   via ::, 00:26:01, vlan3
B 2001:7::/64 [200/0]
   via 2::2, 00:03:21, vlan2
B 2001:8::/64 [200/0]
   via 2::2, 00:02:57, vlan2
```

It can be seen that both 2001:7::/64 and 2001:8::/64 on Device1 select Device2 as the optimal next hop device.

## #View the routing table of Device 4.

```
Device4#show bgp ipv6 unicast
BGP table version is 4, local router ID is 4.4.4.4
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop        Metric   LocPrf Weight Path
[B]* 2001:1::/64  2001:6::2       0         0 100 i
[B]*> 2001:5::2   2001:5::2       0         0 100 i
[B]* 2001:2::/64  2001:6::2       0         0 100 i
[B]*> 2001:5::2   2001:5::2       0         0 100 i
[B]*> 2001:7::/64  ::              0        32768 i
[B]*> 2001:8::/64  ::              0        32768 i

Device4#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
```

U - Per-user Static route  
O - OSPF, OE-OSPF External, M - Management

```
L ::1/128 [0/0]
  via ::, 1w5d:04:14:15, lo0
B 2001:1::/64 [20/0]
  via 2001:5::2, 00:06:52, vlan2
B 2001:2::/64 [20/0]
  via 2001:5::2, 00:06:52, vlan2
C 2001:5::/64 [0/0]
  via ::, 00:26:17, vlan3
L 2001:5::1/128 [0/0]
  via ::, 00:26:16, vlan3
C 2001:6::/64 [0/0]
  via ::, 00:26:24, vlan2
L 2001:6::1/128 [0/0]
  via ::, 00:26:23, vlan2
C 2001:7::/64 [0/0]
  via ::, 00:25:53, vlan4
L 2001:7::1/128 [0/0]
  via ::, 00:25:51, vlan4
C 2001:8::/64 [0/0]
  via ::, 00:25:40, vlan5
L 2001:8::1/128 [0/0]
  via ::, 00:25:40, vlan5
```

According to the result, both 2001:1::/64 and 2001:2::/64 on Device4 select Device3 as the optimal next hop device.

Step 4: Configure access control list and routing policy, and set local-preference and metric.

#Configure Device2.

```
Device2(config)#ipv6 access-list extended 7001
Device2(config-v6-list)#permit ipv6 2001:8::/64 any
Device2(config-v6-list)#commit
Device2(config-v6-list)#exit
Device2(config)#ipv6 access-list extended 7002
Device2(config-v6-list)#permit ipv6 2001:1::/64 any
Device2(config-v6-list)#commit
Device2(config-v6-list)#exit
Device2(config)#route-map SetPriority1 10
Device2(config-route-map)#match ipv6 address 7001
Device2(config-route-map)#set local-preference 110
Device2(config-route-map)#exit
Device2(config)#route-map SetPriority1 20
Device2(config-route-map)#set local-preference 20
Device2(config-route-map)#exit
Device2(config)#route-map SetPriority2 10
Device2(config-route-map)#match ipv6 address 7002
Device2(config-route-map)#set metric 100
Device2(config-route-map)#exit
Device2(config)#route-map SetPriority2 20
Device2(config-route-map)#set metric 20
Device2(config-route-map)#exit
```

Configure routing policy on Device2 to set the local-preference of 2001:8::/64 as 110 and the metric of 2001:1::/64 as 100.

#Configure Device3.

```
Device3(config)#ipv6 access-list extended 7001
Device3(config-v6-list)#permit ipv6 2001:7::/64 any
Device3(config-v6-list)#commit
Device3(config-v6-list)#exit
Device3(config)#ipv6 access-list extended 7002
```

```

Device3(config-v6-list)#permit ipv6 2001:2::/64 any
Device3(config-v6-list)#commit
Device3(config-v6-list)#exit
Device3(config)#route-map SetPriority1 10
Device3(config-route-map)#match ipv6 address 7001
Device3(config-route-map)#set local-preference 110
Device3(config-route-map)#exit
Device3(config)#route-map SetPriority1 20
Device3(config-route-map)#exit
Device3(config)#route-map SetPriority2 10
Device3(config-route-map)#match ipv6 address 7002
Device3(config-route-map)#set metric 100
Device3(config-route-map)#exit
Device3(config)#route-map SetPriority2 20
Device3(config-route-map)#exit

```

Configure routing policy on Device3 to set the local-preference of 2001:7::/64 as 110 and the metric of 2001:2::/64 as 100.

---

## Note

- When configuring a routing policy, both the prefix list and ACL can create filtering rules. The difference is that the prefix list can exactly match the routing mask.
- 

Step 5: Configure IPv6 BGP to associate routing policy.

#Configure Device2.

```

Device2(config)#router bgp 100
Device2(config-bgp)#address-family ipv6
Device2(config-bgp-af)#neighbor 1::1 route-map SetPriority1 out
Device2(config-bgp-af)#neighbor 2001:5::1 route-map SetPriority2 out
Device2(config-bgp-af)#exit-address-family
Device2(config-bgp)#exit

```

On Device2, modify the local-preference of 2001:8::/64 in the outgoing direction of neighbor 1::1 and the metric of 2001:1::/64 in the outgoing direction of neighbor 2001:5::1.

#Configure Device3.

```

Device3(config)#router bgp 100
Device3(config-bgp)#address-family ipv6
Device3(config-bgp-af)#neighbor 1::1 route-map SetPriority1 out
Device3(config-bgp-af)#neighbor 2001:6::1 route-map SetPriority2 out
Device3(config-bgp-af)# exit-address-family
Device2(config-bgp)#exit

```

On Device3, modify the local-preference of 2001:7::/64 in the outgoing direction of neighbor 10.0.0.1 and the metric of 2001:2::/64 in the outgoing direction of neighbor 2001:6::1.

After configuring routing policy on the neighbor, it is required to reset the neighbor to make it take effect.

Step 6: Check the result.

#View the routing table of Device1.

```

Device1#show bgp ipv6 unicast
BGP table version is 9, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
  Network        Next Hop      Metric  LocPrf Weight Path
[B]*> 2001:1::/64  ::           0      32768 i
[B]*> 2001:2::/64  ::           0      32768 i
[B]* i2001:7::/64  2::2        0      100   0 200 i
[B]*>i           3::3        0      110   0 200 i
[B]*>i2001:8::/64  2::2        0      110   0 200 i
[B]* i           3::3        0      100   0 200 i

Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

```

```

L ::1/128 [0/0]
  via ::, 1w5d:04:59:59, lo0
LC 1::1/128 [0/0]
  via ::, 01:05:27, loopback0
O 2::2/128 [110/2]
  via fe80::201:7aff:fe5e:87da, 00:58:52, vlan2
O 3::3/128 [110/2]
  via fe80::201:7aff:fec0:525b, 00:57:26, vlan3
C 2001:1::/64 [0/0]
  via ::, 01:06:00, vlan5
L 2001:1::1/128 [0/0]
  via ::, 01:05:59, vlan5
C 2001:2::/64 [0/0]
  via ::, 01:05:14, vlan4
L 2001:2::1/128 [0/0]
  via ::, 01:05:14, vlan4
C 2001:3::/64 [0/0]
  via ::, 01:05:49, vlan2
L 2001:3::1/128 [0/0]
  via ::, 01:05:48, vlan2
C 2001:4::/64 [0/0]
  via ::, 01:05:43, vlan3
L 2001:4::1/128 [0/0]
  via ::, 01:05:41, vlan3
B 2001:7::/64 [200/0]
  via 3::3, 00:09:05, vlan3
B 2001:8::/64 [200/0]
  via 2::2, 00:04:58, vlan2

```

It can be seen that the local-preference values of 2001:7::/64 and 2001:8::/64 have been successfully modified, and Device1 prefers the route 2001:8::/64 advertised by Device2 and the route 2001:7::/64 advertised by Device3.

#View the routing table of Device 4.

```

Device4#show bgp ipv6 unicast
BGP table version is 5, local router ID is 4.4.4.4
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
  Network        Next Hop      Metric  LocPrf Weight Path
[B]* 2001:1::/64  2001:5::2    100     0 100 i
[B]*>           2001:6::2    0        0 100 i
[B]*> 2001:2::/64  2001:5::2    0        0 100 i
[B]*           2001:6::2    100     0 100 i
[B]*> 2001:7::/64  ::           0      32768 i
[B]*> 2001:8::/64  ::           0      32768 i

Device4#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS

```

U - Per-user Static route  
O - OSPF, OE-OSPF External, M - Management

```
L ::1/128 [0/0]
  via ::, 1w5d:04:53:45, lo0
B 2001:1::/64 [20/0]
  via 2001:6::2, 00:12:10, vlan3
B 2001:2::/64 [20/0]
  via 2001:5::2, 00:07:40, vlan2
C 2001:5::/64 [0/0]
  via ::, 01:05:47, vlan3
L 2001:5::1/128 [0/0]
  via ::, 01:05:46, vlan3
C 2001:6::/64 [0/0]
  via ::, 01:05:54, vlan2
L 2001:6::1/128 [0/0]
  via ::, 01:05:52, vlan2
C 2001:7::/64 [0/0]
  via ::, 01:05:22, vlan4
L 2001:7::1/128 [0/0]
  via ::, 01:05:21, vlan4
C 2001:8::/64 [0/0]
  via ::, 01:05:09, vlan5
L 2001:8::1/128 [0/0]
  via ::, 01:05:09, vlan5
```

It can be seen that the metric values of 2001:1::/64 and 2001:2::/64 have been successfully modified, and Device4 prefers the route 2001:2::/64 advertised by Device2 and the route 2001:1::/64 advertised by Device3.

---

### Note

- Routing policy can be used either in the outgoing direction of route advertisement or in the incoming direction of route receiving.
- 

## 61.3.7 Configure coordination of IPv6 BGP with BFD

### Network Requirements

- Device1 establishes EBGP neighbors with Device2 and Device3, and IBGP neighbors are established between Device2 and Device3.
- Device1 learns the EBGP route 2001:3::/64 from Device2 and Device3 at the same time, and prefers Device2 to forward data to the network segment 2001:3::/64.
- Configure EBGP to associate BFD on Device1 and Device2. When the line between Device1 and Device2 fails, BFD can quickly detect and notify BGP. Then, Device1 chooses Device3 to forward data to the network segment 2001:3::/64.

### Network Topology

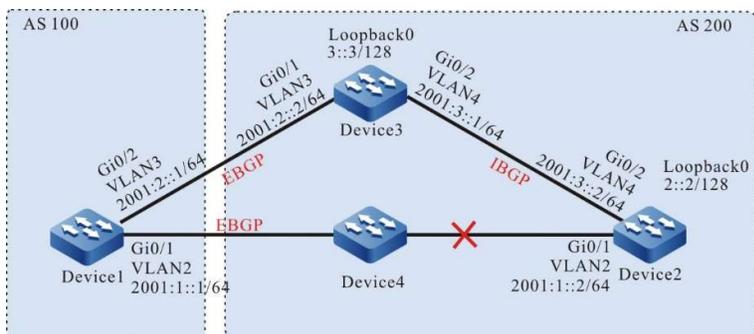


Figure 61 Network Topology for Configuring Coordination of IPv6 BGP with BFD

## Configuration Steps

Step 1: Configure IPv6 global unicast address for interface. (Omitted)

Step 2: Configure OSPFv3 so that the routes of Loopback interfaces between devices are reachable from each other.

### #Configure Device2.

```
Device2#configure terminal
Device2(config)#ipv6 router ospf 100
Device2(config-ospf6)#router-id 2.2.2.2
Device2(config-ospf6)#exit
Device2(config)# interface vlan 4
Device2(config-if-vlan4)#ipv6 router ospf 100 area 0
Device2(config-if-vlan4)#exit
Device2(config)#interface loopback 0
Device2(config-if-loopback0)#ipv6 router ospf 100 area 0
Device2(config-if-loopback0)#exit
```

### #Configure Device3.

```
Device3#configure terminal
Device3(config)#ipv6 router ospf 100
Device3(config-ospf6)#router-id 3.3.3.3
Device3(config-ospf6)#exit
Device3(config)#interface vlan 4
Device3(config-if-vlan4)#ipv6 router ospf 100 area 0
Device3(config-if-vlan4)#exit
Device3(config)# interface loopback 0
Device3(config-if-loopback0)#ipv6 router ospf 100 area 0
Device3(config-if-loopback0)#exit
```

### #View the routing table of Device 2.

```
Device2#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
  via ::, 1w2d:09:31:22, lo0
LC 2::2/128 [0/0]
  via ::, 00:10:10, loopback0
O 3::3/128 [110/1]
  via fe80::201:7aff:fec0:525a, 00:00:12, vlan4
C 2001:1::/64 [0/0]
  via ::, 00:10:54, vlan2
```

```

L 2001:1::2/128 [0/0]
  via ::, 00:10:53, vlan2
C 2001:3::/64 [0/0]
  via ::, 00:10:17, vlan4
L 2001:3::2/128 [0/0]
  via ::, 00:10:16, vlan4

```

### #Check the routing table of Device3.

```

Device3#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
  via ::, 1w6d:03:50:38, lo0
O 2::2/128 [110/2]
  via fe80::201:7aff:fe5e:6d2e, 00:02:40, vlan4
LC 3::3/128 [0/0]
  via ::, 00:00:49, loopback0
C 2001:2::/64 [0/0]
  via ::, 00:03:03, vlan3
L 2001:2::2/128 [0/0]
  via ::, 00:03:02, vlan3
C 2001:3::/64 [0/0]
  via ::, 00:03:18, vlan4
L 2001:3::1/128 [0/0]
  via ::, 00:03:17, vlan4

```

It can be seen that Device2 and Device3 can learn the routes of their loopback interface from each other.

Step 3: Configure access control list and routing policy, and set the routing metric.

### #Configure Device1.

```

Device1#configure terminal
Device1(config)#ipv6 access-list extended 7001
Device1(config-v6-list)#permit ipv6 2001:3::/64 any
Device1(config-v6-list)#commit
Device1(config-v6-list)#exit
Device1(config)#route-map SetMetric
Device1(config-route-map)#match ipv6 address 7001
Device1(config-route-map)#set metric 50
Device1(config-route-map)#exit

```

On Device1, configure the routing policy and set the metric value of 2001:3::/64 as 50.

Step 4: Configure basic functions of IPv6 BGP and associate routing policy on Device1.

### #Configure Device1.

```

Device1(config)#router bgp 100
Device1(config-bgp)#bgp router-id 1.1.1.1
Device1(config-bgp)#address-family ipv6
Device1(config-bgp-af)#neighbor 2001:1::2 remote-as 200
Device1(config-bgp-af)#neighbor 2001:2::2 remote-as 200
Device1(config-bgp-af)#neighbor 2001:2::2 route-map SetMetric in
Device1(config-bgp-af)#exit-address-family
Device1(config-bgp)#exit

```

### #Configure Device2.

```

Device2(config)#router bgp 200
Device2(config-bgp)#bgp router-id 2.2.2.2
Device2(config-bgp)#address-family ipv6

```

```

Device2(config-bgp-af)#neighbor 2001:1::1 remote-as 100
Device2(config-bgp-af)#neighbor 3::3 remote-as 200
Device2(config-bgp-af)#network 2001:3::/64
Device2(config-bgp-af)#exit-address-family
Device2(config-bgp)#neighbor 3::3 update-source loopback 0
Device2(config-bgp)#exit

```

### #Configure Device3.

```

Device3(config)#router bgp 200
Device3(config-bgp)#bgp router-id 3.3.3.3
Device3(config-bgp)#address-family ipv6
Device3(config-bgp-af)#neighbor 2001:2::1 remote-as 100
Device3(config-bgp-af)#neighbor 2::2 remote-as 200
Device3(config-bgp-af)#network 2001:3::/64
Device3(config-bgp-af)#exit-address-family
Device3(config-bgp)#neighbor 2::2 update-source loopback 0
Device3(config-bgp)#exit

```

After configuring routing policy on the peer, it is required to reset the peer to make it take effect.

### #View the status of IPv6 BGP neighbors on Device1.

```

Device1#show bgp ipv6 unicast summary
BGP router identifier 1.1.1.1, local AS number 100
BGP table version is 2
2 BGP AS-PATH entries
0 BGP community entries

Neighbor    V  AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State/PfxRed
2001:1::2   4 200   7    6    2    0 00:04:00   1
2001:2::2   4 200   5    5    2    0 00:02:03   1

Total number of neighbors 2

```

### #View the status of IPv6 BGP neighbors on Device 2.

```

Device2#show bgp ipv6 unicast summary
BGP router identifier 2.2.2.2, local AS number 200
BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries

Neighbor    V  AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State/PfxRed
3::3       4 200   5    5    2    0 00:02:10   1
2001:1::1   4 100   6    7    2    0 00:04:38   0

Total number of neighbors 2

```

According to the result, IPv6 BGP neighbor has been successfully established between Device1, Device2 and Device3.

### #View the routing table of Device1.

```

Device1#show bgp ipv6 unicast
BGP table version is 2, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Network      Next Hop      Metric  LocPrf Weight Path
[B]* 2001:3::/64 2001:2::2     50      0 200 i
[B]*>      2001:1::2     0        0 200 i

Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

```

```

L ::1/128 [0/0]
  via ::, 1w2d:09:53:27, lo0
C 2001:1::/64 [0/0]
  via ::, 00:24:05, vlan2
L 2001:1::1/128 [0/0]
  via ::, 00:24:02, vlan2
C 2001:2::/64 [0/0]
  via ::, 00:25:21, vlan3
L 2001:2::1/128 [0/0]
  via ::, 00:25:20, vlan3
B 2001:3::/64 [20/0]
  via 2001:1::2, 00:05:06, vlan2

```

According to the result, the route 2001:3::/64 on Device1 selects Device2 as the optimal next hop device.

Step 5: Configure coordination of IPv6 BGP with BFD.

#Configure Device1.

```

Device1(config)#router bgp 100
Device1(config-bgp)#address-family ipv6
Device1(config-bgp-af)#neighbor 2001:1::2 fall-over bfd
Device1(config-bgp-af)#exit-address-family
Device1(config-bgp)#exit
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#bfd min-transmit-interval 500
Device1(config-if-vlan2)#bfd min-receive-interval 500
Device1(config-if-vlan2)#bfd multiplier 4
Device1(config-if-vlan2)#exit

```

#Configure Device2.

```

Device2(config)#router bgp 200
Device2(config-bgp)#address-family ipv6
Device2(config-bgp-af)#neighbor 2001:1::1 fall-over bfd
Device2(config-bgp-af)#exit-address-family
Device2(config-bgp)#exit
Device2(config)#interface vlan 2
Device2(config-if-vlan2)#bfd min-transmit-interval 500
Device2(config-if-vlan2)#bfd min-receive-interval 500
Device2(config-if-vlan2)#bfd multiplier 4
Device2(config-if-vlan2)#exit

```

Enable BFD between Device1 and Device2, and modify BFD to control the minimum sending interval, minimum receiving interval and detection timeout multiples of packets.

Step 6: Check the result.

#View the BFD session status on Device1.

```

Device1#show bfd session ipv6
OurAddr          NeighAddr          State  Holddown  Interface
2001:1::1        2001:1::2          UP     2000      vlan2

```

According to the result, BFD status on Device1 is correctly up, and the holddown time is negotiated as 2000ms.

#When the lines between Device1 and Device2 fail, the route can quickly switch to the backup line.

#View the routing table of Device1.

```

Device1#show bgp ipv6 unicast
BGP table version is 3, local router ID is 1.1.1.1

```

Status codes: s suppressed, d damped, h history, \* valid, > best, i - internal,  
 S Stale  
 Origin codes: i - IGP, e - EGP, ? - incomplete  
 Network Next Hop Metric LocPrf Weight Path  
**[B]\*> 2001:3::/64 2001:2::2 50 0 200 i**  
 Device1#show ipv6 route  
 Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS  
 U - Per-user Static route  
 O - OSPF, OE-OSPF External, M - Management

```
L ::1/128 [0/0]
  via ::, 1w2d:10:06:30, lo0
C 2001:1::/64 [0/0]
  via ::, 00:37:08, vlan2
L 2001:1::1/128 [0/0]
  via ::, 00:37:04, vlan2
C 2001:2::/64 [0/0]
  via ::, 00:38:24, vlan3
L 2001:2::1/128 [0/0]
  via ::, 00:38:23, vlan3
B 2001:3::/64 [20/0]
  via 2001:2::2, 00:00:16, vlan3
```

It can be seen that the next hop of 2001 :3 ::/64 switches to Device3.

## 61.3.8 Configure IPv6 BGP static FRR

### Network Requirements

- All devices are configured with IPv6 BGP protocol.
- Enable static FRR between Device1 and Device3. When the lines fail, the service can quickly switch to Device2 for communication.

### Network Topology

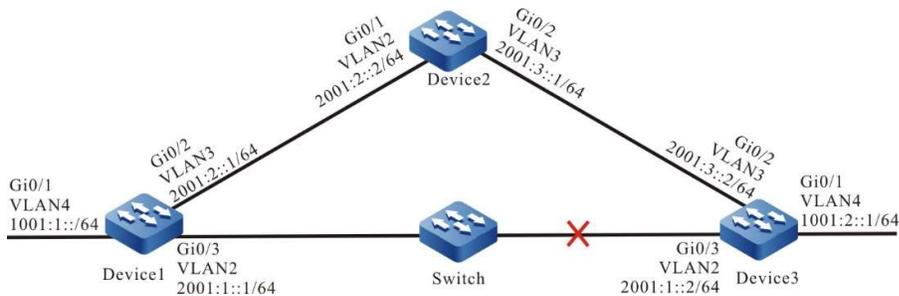


Figure 2 Network Topology for Configuring IPv6 BGP Static FRR

### Configuration Steps

Step 1: Configure VLAN, and add ports to the required VLAN; configure the IPv6 address of each interface (Omitted).

```
S      Configure BGP.  
t  
e  
p  
2  
:
```

#Device1 establishes BGP neighbors with Device2 and Device3.

```
Device1(config)#router bgp 100  
Device1(config-bgp)#bgp router-id 1.1.1.1  
Device1(config-bgp)#address-family ipv6  
Device1(config-bgp-af)#neighbor 2001:1::2 remote-as 300  
Device1(config-bgp-af)#neighbor 2001:2::2 remote-as 200  
Device1(config-bgp-af)#exit-address-family  
Device1(config-bgp)#exit
```

#Device2 establishes BGP neighbors with Device1 and Device3.

```
Device2(config)#router bgp 200  
Device2(config-bgp)#bgp router-id 2.2.2.2  
Device2(config-bgp)#address-family ipv6  
Device2(config-bgp-af)#neighbor 2001:2::1 remote-as 100  
Device2(config-bgp-af)#neighbor 2001:3::2 remote-as 300  
Device2(config-bgp-af)#exit-address-family  
Device2 (config-bgp)#exit
```

#Device3 establishes BGP neighbors with Device1 and Device2.

```
Device3(config)#router bgp 300
Device3(config-bgp)#bgp router-id 3.3.3.3
Device3(config-bgp)#address-family ipv6 unicast
Device3(config-bgp-af)#neighbor 2001:3::1 remote-as 200
Device3(config-bgp-af)#neighbor 2001:1::1 remote-as 100
Device3(config-bgp-af)#network 1001:2::/64
Device3(config-bgp-af)#exit-address-family
Device3(config-bgp)#exit
```

```
S      Configure routing policy.
t
e
p
3
:
```

#On Device1, configure route-map to invoke ACL to match 1001:2::1/64 only, and filter other network segments. The route matching the match rule applies the backup next hop interface vlan3. The next hop address is 2001:2::2.

```
Device1(config)#ipv6 access-list extended 7001
Device1(config-v6-list)#permit ipv6 1001:2::1/64 any
Device1(config-v6-list)#exit
Device1(config)#route-map ipv6frr_bgp
Device1(config-route-map)#match ipv6 address 7001
Device1(config-route-map)#set ipv6 fast-reroute backup-interface vlan3 backup-next-hop 2001:2::2
Device1(config-route-map)#exit
```

```
S      Configure static FRR.
t
e
p
4
:
```

```
Device1(config)#router bgp 100
Device1(config-bgp)#address-family ipv6 unicast
Device1(config-bgp-af)#fast-reroute route-map ipv6frr_bgp
Device1(config-bgp-af)#exit-address-family
Device1(config-bgp)#exit
```

```
S      Check the results.
t
e
p
5
:
```

#View the IPv6 BGP routing table of Device1.

```
Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management
L ::1/128 [0/0]
  via ::, 23:12:10, lo0
C 1001:1::/64 [0/0]
  via ::, 23:07:17, vlan4
```

```

L 1001:1::1/128 [0/0]
  via ::, 23:07:17, vlan4
B 1001:2::/64 [20/0]
  via 2001:1::2, 00:03:25, vlan2
C 2001:1::/64 [0/0]
  via ::, 13:47:06, vlan2
L 2001:1::1/128 [0/0]
  via ::, 13:47:06, vlan2
C 2001:2::/64 [0/0]
  via ::, 23:06:35, vlan3
L 2001:2::1/128 [0/0]
  via ::, 23:06:35, vlan3

```

According to the routing table, the route 1001:2::/64 prefers the lines between Device1 and Device3 for communication.

#View IPv6 FRR routing table on Device1.

```

Device1#show ipv6 frr route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management
B 1001:2::/64 [20/4294967295]
  via 2001:2::2, 00:05:16, vlan3

```

According to the result, the next hop and output interface of the frr route 1001:2::/64 are 2001:2::2 and vlan3 respectively.

#View the BFD session information of Device1.

```

Device1#show bfd session ipv6 2001:1::1 detail
Total ipv6 session number: 1
OurAddr      NeighAddr      LD/RD          State  Holddown  Interface
2001:1::1    2001:1::1      1016/1016      UP     500       vlan2
Type:ipv6 direct Mode:echo
Local Discriminator:73 Remote Discriminator:73
Local State:UP Remote State:UP Up for: 0h:8m:52s Number of times UP:1
Send Interval:100ms Detection time:500ms(100ms*5)
Local Diag:0 Demand mode:0 Poll bit:0
Registered modules:FIB_MGR

```

According to the result, FIB\_MGR has been successfully coordinated with BFD. The session is established normally in the mode of echo.

#When the lines between Device1 and Device3 fail, it can quickly identify the failures and switch to Device2 for communication. The routing table of Device1 shows that the output interface of the destination network 1001:2::/64 has switched to the backup interface vlan3.

```

Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management
L ::1/128 [0/0]
  via ::, 23:18:47, lo0
C 1001:1::/64 [0/0]
  via ::, 23:13:54, vlan4
L 1001:1::1/128 [0/0]
  via ::, 23:13:54, vlan4
B 1001:2::/64 [20/0]
  via 2001:2::2, 00:00:03, vlan3
C 2001:2::/64 [0/0]
  via ::, 23:13:12, vlan3
L 2001:2::1/128 [0/0]
  via ::, 23:13:12, vlan3

```

## 61.3.9 Configure IPv6 BGP dynamic FRR

### Network Requirements

- All devices are configured with IPv6 BGP protocol.
- Enable dynamic FRR between Device1 and Device3. When the lines fail, the service can quickly switch to Device2 for communication.

### Network Topology

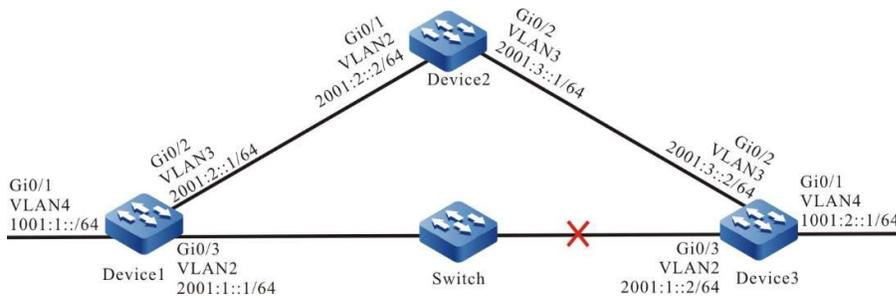


Figure 61 Network Topology for Configuring IPv6 BGP Dynamic FRR

### Configuration Steps

Step 1: Configure VLAN, and add ports to the required VLAN; configure the IPv6 address of each interface (Omitted).

```
S      Configure BGP.  
t  
e  
p  
2  
:
```

#Device1 establishes BGP neighbors with Device2 and Device3.

```
Device1(config)#router bgp 100  
Device1(config-bgp)#bgp router-id 1.1.1.1  
Device1(config-bgp)#address-family ipv6  
Device1(config-bgp-af)#neighbor 2001:1::2 remote-as 300  
Device1(config-bgp-af)#neighbor 2001:2::2 remote-as 200  
Device1(config-bgp-af)#exit-address-family  
Device1(config-bgp)#exit
```

#Device2 establishes BGP neighbors with Device1 and Device3.

```
Device2(config)#router bgp 200  
Device2(config-bgp)#bgp router-id 2.2.2.2  
Device2(config-bgp)#address-family ipv6  
Device2(config-bgp-af)#neighbor 2001:2::1 remote-as 100  
Device2(config-bgp-af)#neighbor 2001:3::2 remote-as 300  
Device2(config-bgp-af)#exit-address-family  
Device2 (config-bgp)#exit
```

#Device3 establishes BGP neighbors with Device1 and Device2.

```
Device3(config)#router bgp 300
Device3(config-bgp)#bgp router-id 3.3.3.3
Device3(config-bgp)#address-family ipv6 unicast
Device3(config-bgp-af)#neighbor 2001:3::1 remote-as 200
Device3(config-bgp-af)#neighbor 2001:1::1 remote-as 100
Device3(config-bgp-af)#network 1001:2::/64
Device3(config-bgp-af)#exit-address-family
Device3(config-bgp)#exit
```

```
S      Configure routing policy.
t
e
p
3
:
```

#On Device1, configure route-map to invoke ACL to match 1001:2::1/64 only, and filter other network segments. The route matching the match rule applies the backup next hop interface vlan3. The next hop address is 2001:2::2.

```
Device1(config)#ipv6 access-list extended 7001
Device1(config-v6-list)#permit ipv6 1001:2::1/64 any
Device1(config-v6-list)#exit
Device1(config)#route-map ipv6frr_bgp
Device1(config-route-map)#match ipv6 address 7001
Device1(config-route-map)# set ipv6 fast-reroute backup-nexthop auto
Device1(config-route-map)#exit
```

```
S      Configure static FRR.
t
e
p
4
:
```

```
Device1(config)#router bgp 100
Device1(config-bgp)#address-family ipv6 unicast
Device1(config-bgp-af)#fast-reroute route-map ipv6frr_bgp
Device1(config-bgp-af)#exit-address-family
Device1(config-bgp)#exit
```

```
S      Check the results.
t
e
p
5
:
```

#View the IPv6 BGP routing table of Device1.

```
Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management
L ::1/128 [0/0]
  via ::, 23:12:10, lo0
C 1001:1::/64 [0/0]
  via ::, 23:07:17, vlan4
L 1001:1::1/128 [0/0]
```

```

    via ::, 23:07:17, vlan4
B 1001:2::/64 [20/0]
  via 2001:1::2, 00:03:25, vlan2
C 2001:1::/64 [0/0]
  via ::, 13:47:06, vlan2
L 2001:1::1/128 [0/0]
  via ::, 13:47:06, vlan2
C 2001:2::/64 [0/0]
  via ::, 23:06:35, vlan3
L 2001:2::1/128 [0/0]
  via ::, 23:06:35, vlan3

```

According to the routing table, the route 1001:2::/64 prefers the lines between Device1 and Device3 for communication.

#View IPv6 FRR routing table on Device1.

```

Device1#show ipv6 frr route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management
B 1001:2::/64 [20/4294967295]
  via 2001:2::2, 00:05:16, vlan3

```

According to the result, the next hop and output interface of the frr route 1001:2::/64 are 2001:2::2 and vlan3 respectively.

#View the BFD session information of Device1.

```

Device1#show bfd session ipv6 2001:1::1 detail
Total ipv6 session number: 1
OurAddr      NeighAddr      LD/RD          State  Holddown  Interface
2001:1::1    2001:1::1      1032/1032     UP     500       vlan2
Type:ipv6 direct Mode:echo
Local Discriminator:73 Remote Discriminator:73
Local State:UP Remote State:UP Up for: 0h:8m:52s Number of times UP:1
Send Interval:100ms Detection time:500ms(100ms*5)
Local Diag:0 Demand mode:0 Poll bit:0
Registered modules:FIB_MGR

```

According to the result, FIB\_MGR has been successfully coordinated with BFD. The session is established normally in the mode of echo.

#When the lines between Device1 and Device3 fail, it can quickly identify the failures and switch to Device2 for communication. The routing table of Device1 shows that the output interface of the destination network 1001:2::/64 has switched to the backup interface vlan3.

```

Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management
L ::1/128 [0/0]
  via ::, 23:18:47, lo0
C 1001:1::/64 [0/0]
  via ::, 23:13:54, vlan4
L 1001:1::1/128 [0/0]
  via ::, 23:13:54, vlan4
B 1001:2::/64 [20/0]
  via 2001:2::2, 00:00:03, vlan3
C 2001:2::/64 [0/0]
  via ::, 23:13:12, vlan3
L 2001:2::1/128 [0/0]
  via ::, 23:13:12, vlan3

```

# 62 Policy Route

---

## 62.1 Overview

Policy route is a routing mechanism which conducts packet forwarding according to users' customized policies. When forwarding routes, the packet can be matched according to ACL rules. The content to be matched includes IP protocol number, source IP address, destination IP address, source TCP/UDP port number, destination TCP/UDP port number, packet priority, and TCP flag. For the packets that meet the match rules, corresponding operations shall be conducted according to the specified policy (set next hop of the packet) to complete their forwarding control.

The traditional routing method forwards packets according to destination address. By contrast, policy route is more flexible. It effectively complements and reinforces the traditional routing mechanism.

## 62.2 Function configuration of policy route

Table 62 Policy Route Configuration List

Configuration Task	
Configure Policy Route	Configure Next Hop IP Address for Packet Forwarding
	Configure Backup Next Hop IP Address for Packet Forwarding
	Configure Next Hop IPv6 Address for Packet Forwarding
	Configure Backup Next Hop IPv6 Address for Packet Forwarding
	Configure Binding of PBR Action Group to ACL

Configuration Task	
	Configure Binding of PBR Action Group to ACL Rules
Configuration Application of Policy Route	Configure Application of ACL with Policy Route to Layer-2/3 Ethernet Interface
	Configure Application of ACL with Policy Route to VLAN
	Configure Application of ACL with Policy Route to Interface VLAN
	Configure Application of ACL with Policy Route to vlan range
	Configure Application of ACL with Policy Route to interface vlan range
	Configure Application of ACL with Policy Route to global

### 62.2.1 Configure Policy Route

The implementation of policy route depends on the filtration of packets by ACL rules. The ACL rules first filter out the packets that meet the conditions, and then execute policy route forwarding to the next hop for the packets.

#### Configuration Condition

Before configuring the functions of policy route, ensure that:

- Configure ACL and ACL rules.

#### Configure Next Hop IP Address for Packet Forwarding

Configure the next hop IP address for packet forwarding to specify the destination address of policy route.

At most 6 next hop IP addresses for packet forwarding can be configured. If users configure multiple next hop IP addresses simultaneously and there are several reachable next hop IP addresses, the packet will be forwarded to the next hop IP address through load balancing.

Table 62 Configuring Next Hop IP Address for Packet Forwarding

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter PBR action group configuration mode	<b>pbr-action-group</b> <i>pbr-action-group-name</i>	-
Configure next hop IP address for packet forwarding	<b>redirect ipv4-nexthop</b> <i>ip-address [ip-address] [ip-address] [ip-address] [ip-address] [vrf vrf-name]</i>	Mandatory  By default, the next hop IP address for packet forwarding is not configured.

### Note

- If all the next hop IP addresses configured for forwarding are not reachable, the function of policy route will not take effect.
- The next hop IP address shall not be configured as multicast address or broadcast address.
- The device doesn't support ECMP load balancing. The traffic always pass through the first effective next hop.

### Configure Backup Next Hop IP Address for Packet Forwarding

Configure the backup next hop IP address for packet forwarding to specify the destination address of policy route.

When the primary next hop is unreachable, if the backup next hop IP address is reachable, the packet is forwarded to the backup next hop IP address; if the primary next hop is reachable, the packet continues to be forwarded to such primary next hop IP address.

Table 1 Configuring Backup Next Hop IP Address for Packet Forwarding

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter PBR action group configuration mode	<b>pbr-action-group</b> <i>pbr-action-group-name</i>	-

Step	Command	Description
Configure next hop IP address for packet forwarding	<b>redirect ipv4-nexthop backup</b> <i>ip-address</i> [ <i>vrf vrf-name</i> ]	Mandatory By default, the backup next hop IP address for packet forwarding is not configured.

### Note

- If the backup next hop IP address configured for forwarding is not reachable, the function of policy route will not take effect.
- The next hop IP address shall not be configured as multicast address or broadcast address.

### Configure Next Hop IPv6 Address for Packet Forwarding

Configure the next hop IPv6 address for packet forwarding to specify the destination address of policy route.

At most 6 next hop IPv6 addresses for packet forwarding can be configured. If users configure multiple next hop IPv6 addresses simultaneously and there are several reachable next hop IPv6 addresses, the packet will be forwarded to the next hop IPv6 address through load balancing.

Table 62 Configuring Next Hop IPv6 Address for Packet Forwarding

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter PBR action group configuration mode	<b>pbr-action-group</b> <i>pb-action-group-name</i>	-
Configure next hop IPv6 address for packet forwarding	<b>redirect ipv6-nexthop</b> <i>ipv6-address</i> [ <i>ipv6-address</i> ] [ <i>ipv6-address</i> ] [ <i>ipv6-address</i> ] [ <i>ipv6-address</i> ] [ <i>vrf vrf-name</i> ]	Mandatory By default, the next hop IPv6 address for packet forwarding is not configured.

---

## Note

- If all the next hop IPv6 addresses configured for forwarding are not reachable, the function of policy route will not take effect.
  - The next hop IPv6 address shall not be configured as multicast address or broadcast address.
  - The device doesn't support ECMP load balancing. The traffic always pass through the first effective next hop.
- 

### Configure Backup Next Hop IPv6 Address for Packet Forwarding

Configure the backup next hop IPv6 address for packet forwarding to specify the destination address of policy route.

When the primary next hop is unreachable, if the backup next hop IPv6 address is reachable, the packet is forwarded to the backup next hop IPv6 address; if the primary next hop is reachable, the packet continues to be forwarded to such primary next hop IPv6 address.

Table 62 Configuring Backup Next Hop IPv6 Address for Packet Forwarding

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter PBR action group configuration mode	<b>pbr-action-group</b> <i>pbr-action-group-name</i>	-
Configure next hop IPv6 address for packet forwarding	<b>redirect ipv6-nexthop backup</b> <i>ipv6-address</i> [ <i>vrf vrf-name</i> ]	Mandatory By default, the backup next hop IPv6 address for packet forwarding is not configured.

---

## Note

- If the backup next hop IPv6 address configured for forwarding is not reachable, the function of policy route will not take effect.
  - The next hop IPv6 address shall not be configured as multicast address or broadcast address.
-

## Configure Binding of PBR Action Group to ACL

Configure the binding of PBR action group to ACL so that all ACL rules are associated with actions of policy route.

After the PBR action group is bound to ACL, all ACL rules will associate with actions of policy route. Only if the packets received by the port match the ACL rules, they will be forwarded to the next hop.

Table 62 Configuring Binding of PBR Action Group to ACL

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure Binding of PBR Action Group to ACL	<b>ip pbr-action-group</b> <i>pbr-action-group-name</i> <b>access-list</b> { <i>access-list-number</i>   <i>access-list-name</i> }	Optional By default, PBR action group is not bound to IP ACL.  PBR action group supports the binding of IP ACL which contains standard IP ACL and extended IP ACL.
	<b>ipv6 pbr-action-group</b> <i>pbr-action-group-name</i> <b>access-list</b> { <i>access-list-number</i>   <i>access-list-name</i> }	Optional By default, PBR action group is not bound to IPv6 ACL.  PBR action group supports the binding of IPv6 ACL which contains standard IPv6 ACL and extended IPv6 ACL.

---

### Note

- Only when the next hop IP address configured is reachable will the policy route take effect.
  - The policy route only takes effect for the allowable rules in ACL.
- 

## Configure Binding of PBR Action Group to ACL Rules

Configure the binding of PBR action group to ACL rules so that ACL rules are associated with actions of policy route.

After the PBR action group is bound to ACL rules, ACL rules will associate with actions of policy route. If the packets received by the port match the ACL rules, they will be forwarded according to the next hop specified by the action group.

Table 62 Configuring Binding of PBR Action Group to ACL Rules

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure Binding of PBR Action Group to ACL Rules	Please see "Configure Standard IP ACL" Please see "Configure Extended IP ACL" Please see "Configure Standard IPv6 ACL" Please see "Configure Extended IPv6 ACL"	When configuring the allowable rules of standard IP ACL and extended ACL, you must specify a PBR action group to make the policy route take effect.  When configuring the allowable rules of standard IPv6 ACL and extended ACL, you must specify a PBR action group to make the policy route take effect.

---

 **Note**

- Only when the next hop IP address configured is reachable will the policy route take effect.
  - The policy route only takes effect for the allowable rules in ACL.
- 

### 62.2.2 Configuration Application of Policy Route

The application of policy route is actually that of the ACL with policy route which takes effect depending on ACL rules. ACL can be applied to layer-2/3 Ethernet interface, VLAN, interface VLAN, VLAN RANGE, interface VLAN RANGE, and global.

When the ACL with policy route is applied to global, VLAN, Interface VLAN, VLAN RANGE, Interface VLAN RANGE, and Layer-2/3 Ethernet interface, conflict may appear. In this case, the policy route with a high priority takes effect. The following has the priority from high to low: port, VLAN/ Interface VLAN, VLAN RANGE/Interface VLAN RANGE, global.

## Configuration Condition

None

## Configure Application of ACL with Policy Route to Layer-2/3 Ethernet Interface

After applying the ACL with policy route to layer-2/3 Ethernet interface, corresponding layer-2/3 Ethernet interface will have the function of policy route.

Table 62 Configuring Application of Policy Route to Layer-2/3 Ethernet Interface

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the L2/L3 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2/3 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>link-aggregation</b> <i>link-aggregation-id</i>	
Configuration application of policy route to the port	<b>ip policy-based-route</b> { <i>access-list-number</i>   <i>access-list-name</i> }	Optional  By default, no IP ACL with policy route is applied to the port.
	<b>ipv6 policy-based-route</b> { <i>access-list-number</i>   <i>access-list-name</i> }	Optional  By default, no IPv6 ACL with policy route is applied to the port.

## Configure Application of ACL with Policy Route to VLAN

After applying the ACL with policy route to VLAN, all ports within corresponding VLAN will have the function of policy route.

Table 62 Configuring Application of Policy Route to VLAN

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the VLAN configuration mode	<b>vlan</b> <i>vlan-id</i>	-
Configure application of policy route to VLAN	<b>ip policy-based-route</b> { <i>access-list-number</i>   <i>access-list-name</i> }	Optional By default, no IP ACL with policy route is applied to VLAN.
	<b>ipv6 policy-based-route</b> { <i>access-list-number</i>   <i>access-list-name</i> }	Optional By default, no IPv6 ACL with policy route is applied to VLAN.

### Configure Application of ACL with Policy Route to Interface VLAN

After applying the ACL with policy route to Interface VLAN, corresponding Interface VLAN will have the function of policy route.

Table 62 Configuring Application of Policy Route to Interface VLAN

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the Interface VLAN configuration mode	<b>Interface vlan</b> <i>vlan-id</i>	-
Configure application of policy route to Interface VLAN	<b>ip policy-based-route</b> { <i>access-list-number</i>   <i>access-list-name</i> }	Optional By default, no IP ACL with policy route is applied to Interface VLAN.

Step	Command	Description
	<b>ipv6 policy-based-route</b> { <i>access-list-number</i>   <i>access-list-name</i> }	Optional  By default, no IPv6 ACL with policy route is applied to Interface VLAN.

### Configure Application of ACL with Policy Route to VLAN RANGE

After applying the ACL with policy route to VLAN RANGE, corresponding VLAN RANGE will have the function of policy route.

Table 62 Configuring Application of Policy Route to VLAN RANGE

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure application of policy route to VLAN RANGE	<b>ip policy-based-route</b> { <i>access-list-number</i>   <i>access-list-name</i> } <b>vlan range</b> <1-4094>	Optional  By default, no IP ACL with policy route is applied to VLAN RANGE.
	<b>ipv6 policy-based-route</b> { <i>access-list-number</i>   <i>access-list-name</i> } <b>vlan range</b> <1-4094>	Optional  By default, no IPv6 ACL with policy route is applied to VLAN RANGE.

### Configure Application of ACL with Policy Route to Interface VLAN RANGE

After applying the ACL with policy route to Interface VLAN RANGE, corresponding Interface VLAN RANGE will have the function of policy route.

Table 2 Configuring Application of Policy Route to Interface VLAN RANGE

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Configure application of policy route to VLAN RANGE	<b>ip policy-based-route</b> { <i>access-list-number</i>   <i>access-list-name</i> } <b>interface</b> <b>vlan range</b> <1-4094>	Optional By default, no IP ACL with policy route is applied to Interface VLAN RANGE.
	<b>ipv6 policy-based-route</b> { <i>access-list-number</i>   <i>access-list-name</i> } <b>interface</b> <b>vlan range</b> <1-4094>	Optional By default, no IPv6 ACL with policy route is applied to Interface VLAN RANGE.

### Configure Application of ACL with Policy Route to global

After applying the ACL with policy route to global, all ports of the device will have the function of policy route.

Table 3 Configuring Application of Policy Route to Global

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure application of policy route to global	<b>global ip policy-based-route</b> { <i>access-list-number</i>   <i>access-list-name</i> }	Mandatory By default, no ACL with policy route is applied to global.

### 62.2.3 Policy route monitoring and maintaining

Table 62 Policy Route Monitoring and Maintaining

Command	Description
<b>show pbr-action-group</b> [ <i>pbr-action-group-name</i> ]	Show the configuration information of policy route

Command	Description
<b>show policy-based-route object</b> [ global   interface [ vlan   switchport   vlan-range ]   vlan   vlan-range ]	Show policy route configuration and application information. If no parameter has been specified, then it means the application information of all PBRs.

## 62.3 Typical configuration example of policy route

### 62.3.1 Configure Policy Route

#### Network Requirements

- Device1 has default route. The gateway is Device2.
- By configuring policy route on Device1, the PC can access network 1.1.1.0/24 through Device3, and network 1.1.2.0/24 through Device2.

#### Network Topology

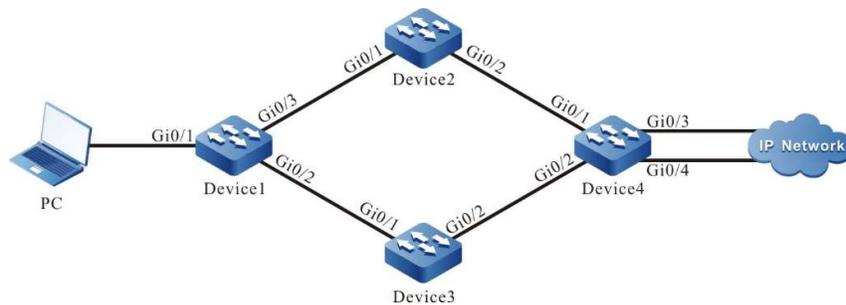


Figure 62 Network Topology for Configuring Policy Route

of equipment	port	VLAN	IP address
PC			10.1.1.1/24
Device1	Gi0/1	2	10.1.1.2/24
	Gi0/2	3	20.1.1.1/24
	Gi0/3	4	30.1.1.1/24
Device2	Gi0/1	2	30.1.1.2/24

of equipment	port	VLAN	IP address
	Gi0/2	3	50.1.1.1/24
Device3	Gi0/1	2	20.1.1.2/24
	Gi0/2	3	40.1.1.1/24
Device4	Gi0/1	2	50.1.1.2/24
	Gi0/2	3	40.1.1.2/24
	Gi0/3	4	1.1.1.1/24
	Gi0/4	5	1.1.2.1/24

### Configuration Steps

Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configures IP addresses for the ports. (Omitted)

Step 3: Configure static routes.

#### #Configure Device1.

```
Device1#configure terminal
Device1(config)#ip route 0.0.0.0 0.0.0.0 30.1.1.2
```

#### #Configure Device2.

```
Device2#configure terminal
Device2(config)#ip route 10.1.1.0 255.255.255.0 30.1.1.1
Device2(config)#ip route 1.1.0.0 255.255.0.0 50.1.1.2
```

#### #Configure Device3.

```
Device3#configure terminal
Device3(config)#ip route 10.1.1.0 255.255.255.0 20.1.1.1
Device3(config)#ip route 1.1.0.0 255.255.0.0 40.1.1.2
```

#### #Configure Device4.

```
Device4#configure terminal
Device4(config)#ip route 30.1.1.0 255.255.255.0 50.1.1.1
Device4(config)#ip route 20.1.1.0 255.255.255.0 40.1.1.1
Device4(config)#ip route 10.1.1.0 255.255.255.0 50.1.1.1
Device4(config)#ip route 10.1.1.0 255.255.255.0 40.1.1.1
```

#### #View the routing table of Device1.

```
Device1#show ip route
```

Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management  
D - Redirect, E - IRMP, Ex - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is 30.1.1.2 to network 0.0.0.0

```
S 0.0.0.0/0 [1/100] via 30.1.1.2, 00:26:24, vlan4
C 10.1.1.0/24 is directly connected, 00:00:59, vlan2
C 20.1.1.0/24 is directly connected, 00:00:50, vlan3
C 30.1.1.0/24 is directly connected, 00:00:39, vlan4
C 127.0.0.0/8 is directly connected, 03:47:36, lo0
```

#### Step 4: Configure policy route on Device1.

#Configure PBR action group, and re-direct the packets to the next hop 20.1.1.2.

```
Device1(config)#pbr-action-group pbr
Device1(config-action-group)#redirect ipv4-nexthop 20.1.1.2
Device1(config-action-group)#exit
```

#View the information of PBR action group on Device1.

```
Device1#show pbr-action-group pbr
pbr-action-group pbr
redirect ipv4-nexthop 20.1.1.2(valid)
```

#Configure ACL, and bind the ACL rules matching the destination IP network segment 1.1.1.0/24 to the L3 PBR action group.

```
Device1(config)#ip access-list extended 1001
Device1(config-std-nacl)#permit ip any 1.1.1.0 0.0.0.255 pbr-action-group pbr
Device1(config-std-nacl)#permit ip any 1.1.2.0 0.0.0.255
Device1(config-std-nacl)#commit
Device1(config-std-nacl)#exit
```

#View the information of ACL on Device1.

```
Device1#show ip access-list 1001
ip access-list standard 1001
10 permit ip any 1.1.1.0 0.0.0.255 pbr-action-group pbr (active)
20 permit ip any 1.1.2.0 0.0.0.255
```

#### Step 6: Apply ACL.

#Apply ACL 1001 to the port vlan2 of Device1.

```
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ip policy-based-route 1001
Device1(config-if-vlan2)#exit
```

#### Step 7: Check the result.

#On the PC, view through Traceroute the paths through which the destination network 1.1.1.0/24 can be reached.

```
C:\Documents and Settings\Administrator>tracert 1.1.1.1
```

Tracing route to 1.1.1.1 over a maximum of 30 hops

```
 1  1 ms  1 ms  1 ms 10.1.1.2
 2 <1 ms <1 ms <1 ms 20.1.1.2
 3 <1 ms <1 ms <1 ms 1.1.1.1
Trace complete.
```

It can be seen that PC reaches network 1.1.1.0/24 through Device1, Device3 and Device4.

#On the PC, view through Traceroute the paths through which the destination network 1.1.2.0/24 can be reached.

```
C:\Documents and Settings\Administrator>tracert 1.1.2.1
```

Tracing route to 1.1.2.1 over a maximum of 30 hops

```
 1  1 ms  1 ms  1 ms 10.1.1.2
 2 <1 ms <1 ms <1 ms 30.1.1.2
 3 <1 ms <1 ms <1 ms 1.1.2.1
Trace complete.
```

It can be seen that PC reaches network 1.1.2.0/24 through Device1, Device2 and Device4.

---

## Note

- The packets can be flexibly matched according to ACL rules referenced. The content to be matched includes packets' source IP address, destination IP address, source port, destination port, protocol, and TCP flag.
  - For ACL binding, except for binding to layer-2/3 Ethernet interface, it can be bound to VLAN, Interface VLAN and global.
-

# 63 Routing Policy Tool

---

## 63.1 Overview

Routing policy changes the paths through which routing information or data traffic passes by changing route attributes or route reachability. It is mainly applied in the following aspects:

- Set route attributes: Set corresponding attributes through the route matching the routing policy;
- Control route distribution: When distributing routes, the routing protocol distributes the routing information which satisfies the conditions only;
- Control route receiving: When receiving routes, the routing protocol receives the routing information which satisfies the conditions only so as to control the number of routing table entries and improve network security;
- Control route redistribution: When redistributing and importing external routes, the routing protocol imports routing information which satisfies the conditions, or uses routing policy tool to set certain attributes of importing external routes.

Key-chain is a password management tool. It provides authentication password when the routing protocol is authenticating protocol packets.

## 63.2 Function configuration of routing policy tool

Table 63 Routing Policy Tool Configuration List

Configuration Task	
Configure Prefix List	Configure Prefix List

Configuration Task	
Configure AS-PATH List	Configure AS-PATH List
Configure List of Community Attributes	Configure List of Community Attributes
Configure List of Extcommunity Attributes	Configure List of Extcommunity Attributes
Configure Routing Map	Create Routing Map
	Configure match Sub-statement of Routing Map
	Configure set Sub-statement of Routing Map
Configure Key-chain	Configure Key-chain

### 63.2.1 Configure Prefix List

#### Configuration Condition

None

#### Configure Prefix List

Prefix list can be used to filter prefixes and particularly routes. ACL is designed to filter data packet at first and routes later. However, prefix list is designed to filter routes. Although they overlap in route filtration, prefix list is more flexible than ACL.

A prefix list is identified with a name of prefix list. Each prefix list can contain multiple entries, each of which can separately specify a match scope. Each entry corresponding to a number is used to indicate the sequence in which the prefix list conducts match check.

The relationship between entries of the prefix list is "or". During the matching process, the device checks according to corresponding sequence number of the entries from small to large. Once a specific entry is matched, the filtration of this prefix list has been passed, and it will not continue to check the next entry.

Table 63 Configuring Prefix List

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure IPv4 prefix list	<b>ip prefix-list</b> <i>prefix-list-name</i> [ <b>seq</b> <i>seq-value</i> ] { <b>deny</b>   <b>permit</b> } <i>network / length</i> [ <b>ge</b> <i>ge-value</i> ] [ <b>le</b> <i>le-value</i> ]	Mandatory  By default, no IPv4 prefix list is configured.

---

### Note

- **ge** means greater than or equal to, and **le** means less than or equal to. The value range is  $0 \leq \text{length} < \text{ge-value} \leq \text{le-value} \leq 32$ . For example, if you configure **ip prefix-list test permit 192.168.0.0/16 ge 18 le 24**, it means that routing entries with an address of 192.168.0.0 and a mask length between 18 (inclusive) and 24 (inclusive) are permitted to pass.
  - When the network/length is configured as 0.0.0.0/0, it means the default route is matched; when it is configured as 0.0.0.0/0 **le 32**, it means all routes are matched.
  - At the end of the IPv4 prefix list, there is an entry which prohibits all: **deny 0.0.0.0/0 le 32**. When deny statement is configured to prohibit some routes, it is recommended to add **permit 0.0.0.0/0 le 32** statement at the end to permit other IPv4 routes to pass.
- 

## 63.2.2 Configure AS-PATH List

### Configuration Condition

None

### Configure AS-PATH List

AS-PATH list can be used to filter AS numbers and BGP routes. The AS path attributes of BGP route record all the AS through which this route passes. When advertising a route to the outside of this AS, BGP will add the AS number to the AS path attributes to record the information of the AS path through which this route passes.

An AS-PATH list may contain multiple entries, the relationship between which is "or". During the matching process, the device checks according to the sequential order. As long as the route passes a certain entry in this AS-PATH list, it is deemed that it passes this AS-PATH list.

Table 63 Configuring AS-PATH List

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure AS-PATH List	<b>ip as-path access-list</b> <i>path-list-number</i> { <b>permit</b>   <b>deny</b> } <i>regular-expression</i>	Mandatory By default, no AS-PATH list is configured.

Regular expressions are used in the AS-PATH list to specify the set of AS attributes that meets the requirements. Regular expression is composed of some general characters and some metacharacters. General characters include letters in upper and lower case and figures; metacharacters have special meanings, as shown in the table below.

Table 63 Meanings of Metacharacters in Regular Expression

SYMBOL	Meaning
.	Match any single character
*	Match the sequence which can follow 0 or more bits in the mode
+	Match the sequence which can follow 1 or more bits in the mode
?	Match the sequence which can follow 0 or 1 bit in the mode
^	Match the start of the input string
\$	Match the end of the input string
–	Match comma, bracket, start and end of character string, and space

SYMBOL	Meaning
[]	Match the single characters in a certain scope
-	Separate the end points in a scope

### 63.2.3 Configure List of Community Attributes

#### Configuration Condition

None

#### Configure List of Community Attributes

Community-list is used to filter the community attributes of route. Generally, a route has two parts, i.e. prefix and route attributes. In particular, route attributes are different among various routing protocols. Generally, there are simple attributes in the IGP protocol, such as metric. BGP has many complicated attributes, including community attributes. Community-list is used to filter these attributes. The community-list filtering result is obtained for the entire route where this community attribute is located. That is to say, if the filtering result is deny, the entire route rather than just this community attribute will be denied.

Community-list has two types, i.e. standard and extended. The standard community-list filters according to local-AS, internet, no-advertise, and no-export of BGP routes; the extcommunity-list uses regular expressions to filter the BGP routes with these community attributes.

For the use of community-list, routing protocols with community attributes can be used directly. Generally, they are often used indirectly by binding the community-list to the routing map and then applying the routing map to the routing protocol.

A community-list may contain multiple entries, the relationship between which is "or". During the matching process, the device checks according to the sequential order. As long as the route passes a certain entry in this community-list, it is deemed that it passes this community-list. When configuring the extcommunity-list, the use of regular expression can refer to the part of configuring AS-PATH list.

Table 63 Configuring Community-list

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Configure standard community-list	<b>ip community-list</b> { <i>community-list-number</i>   <b>standard</b> <i>community-list-name</i> } { <b>permit</b>   <b>deny</b> } [ <i>community-number</i> / <i>aa: nn</i> / <b>local-AS</b> / <b>internet</b> / <b>no-advertise</b> / <b>no-export</b> ]	Mandatory  By default, no standard community-list is configured.
Configure extcommunity-list	<b>ip community-list</b> { <i>community-list-number</i>   <b>expanded</b> <i>community-list-name</i> } { <b>permit</b>   <b>deny</b> } <i>regular-expression</i>	Mandatory  By default, no extcommunity-list is configured.

## 63.2.4 Configure List of Extcommunity Attributes

### Configuration Condition

None

### Configure List of Extcommunity Attributes

Extcommunity-list can be used to filter extcommunity attributes and particularly routes. The nature and application method of extcommunity-list are almost the same as those of community-list. The difference is that the extcommunity attributes are mainly used in MPLS L3VPN. Therefore, extcommunity-list is also mainly used in MPLS L3VPN.

Extcommunity-list has two types, i.e. standard and extended. The standard community-list filters according to Router Target and Site of Origin; the extended extcommunity-list uses regular expressions to filter the BGP routes with these community attributes.

An extcommunity-list may contain multiple entries, the relationship between which is "or". During the matching process, the device checks according to the sequential order. As long as the route passes a certain entry in this extcommunity-list, it is deemed that it passes this extcommunity-list. When configuring the extended extcommunity-list, the use of regular expression can refer to the part of configuring AS-PATH list.

Table 63 Configuring Extcommunity-list

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure standard extcommunity-list	<b>ip extcommunity-list</b> { <i>extcommunity-list-number</i>   <b>standard</b> <i>extcommunity-list-name</i> } { <b>permit</b>   <b>deny</b> } [ <b>rt</b> <i>extcommunity-number</i> / <b>soo</b> <i>extcommunity-number</i> ]	Mandatory  By default, no standard extcommunity-list is configured.
Configure extended extcommunity-list	<b>ip extcommunity-list</b> { <i>extcommunity-list-number</i>   <b>expanded</b> <i>extcommunity-list-name</i> } { <b>permit</b>   <b>deny</b> } <i>regular-expression</i>	Mandatory  By default, no extended extcommunity-list is configured.

### 63.2.5 Configure Routing Map

Routing map is a tool used to match routes and set route attributes. A routing map is composed of several statements, each of which contains some match sub-statements and set sub-statements. The former define the match rules of this statement, while the latter define the actions after passing the match of match sub-statements. The relationship between match sub-statements is "and", i.e. all match sub-statements of this statement must be satisfied.

The relationship between statements of the routing map is "or". During the matching process, the device checks according to corresponding sequence number of the statements from small to large. Once the check of a specific statement is passed, it means this routing map has been matched, and it will not continue to check the next statement. If no statement check has been passed, this routing map is not matched.

#### Configuration Condition

Before configuring a routing map, ensure that:

- Configure the ACL, prefix list, AS-PATH, community-list or extcommunity list required for routing map.

#### Create Routing Map

When creating the routing map, the match mode of its statements can be specified, i.e. **permit** or **deny**:

**permit** specifies the match mode of the statement of the routing map created is permit. The routing entries are allowed to pass and execute the set sub-statements of this statement when they meet all the match sub-statements of this statement. If the routing entries cannot satisfy the match sub-statements of this statement, the next statement of this routing map will be checked;

The word **deny** specifies the match mode of the statements of the routing map created is deny. The routing entries will be denied and check of the next statement will not be conducted only when they meet all the match sub-statements of this statement. The set sub-statement is not performed in **deny** mode.

Table 63 Creating Routing Map

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Create Routing Map	<b>route-map</b> <i>map-name</i> [ { <b>permit</b>   <b>deny</b> } [ <i>seq-number</i> ] ]	Mandatory  By default, no routing map is created.

### Note

- Create a routing map through the command route-map. When only the name of routing map is configured, yet the match mode and statement number are ignored, a statement with the match mode of permit and number of 10 will be added automatically.
- When the routing protocol applies a routing map which is not configured, all the objects will be matched ineffectively.

### Configure match Sub-statement of Routing Map

The relationship between the match sub-statements of the routing map's statements is "and". All the match sub-statements must be satisfied to pass.

Table 63 Creating Match Sub-statements of Routing Map

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enters the routing map configuration mode	<b>route-map</b> <i>map-name</i> [ { <b>permit</b>   <b>deny</b> } [ <i>seq-number</i> ] ]	-
Specify the AS-PATH list which matches the routing map	<b>match as-path</b> <i>path-list-number</i>	Optional  By default, no AS-PATH list which matches the routing map is specified.
Specify the BGP community-list which matches the routing map	<b>match community</b> <i>community-list-number / community-list-name</i> [ <b>exact-match</b> ]	Optional  By default, no BGP community-list which matches the routing map is specified.
Specify the BGP extcommunity-list which matches the routing map	<b>match extcommunity</b> <i>extcommunity-list-number / extcommunity-list-name</i>	Optional  By default, no BGP extcommunity-list which matches the routing map is specified.
Specify the interface which matches the routing map	<b>match interface</b> <i>interface-names</i>	Optional  By default, no interface which matches the routing map is specified.
Specify the route prefix which matches the routing map	<b>match ip address</b> { <i>access-list-number</i>   <i>access-list-name</i>   <b>prefix-list</b> <i>prefix-list-name</i> }	Optional  By default, no route prefix which matches the routing map is specified.

Step	Command	Description
Specify the next hop address which matches the routing map	<b>match ip next-hop</b> { <i>access-list-name</i>   <b>prefix-list</b> <i>prefix-list-name</i> }	Optional By default, no next hop address which matches the routing map is specified.
Specify the source address of route which matches the routing map	<b>match ip route-source</b> { <i>access-list-name</i>   <b>prefix-list</b> <i>prefix-list-name</i> }	Optional By default, no source address of route which matches the routing map is specified.
Specify the metric value which matches the routing map	<b>match metric</b> <i>metric-value</i> [+ <i>offset</i> ]	Optional By default, no metric value which matches the routing map is specified.
Specify the route type which matches the routing map	<b>match route-type</b> { <b>external</b> / <b>interarea</b> / <b>internal</b> / <b>level-1</b> / <b>level-2</b> / <b>nssa-external</b> / <b>type-1</b> / <b>type-2</b> }	Optional By default, no route type which matches the routing map is specified.
Specify the tag value which matches the routing map	<b>match tag</b> <i>tag-value</i>	Optional By default, no tag value which matches the routing map is specified.

---

## Note

- When no match sub-statement is configured in routing map, all the objects can be successfully matched.
  - When there is no ACL and prefix list associated with the match sub-statements, all the objects cannot be successfully matched.
-

## Configure set Sub-statement of Routing Map

Only when the match mode of the routing map is permit and all the match sub-statements are successfully matched, the set operation can be executed. When the match mode is deny, no set operation will be performed.

Table 63 Configure Set Sub-statements of Routing Map

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enters the routing map configuration mode	<b>route-map</b> <i>map-name</i> [ { <b>permit</b>   <b>deny</b> } [ <i>seq-number</i> ] ]	-
Set the AS path attributes of BGP route	<b>set as-path prepend</b> <i>as-path-number</i>	Optional By default, no AS path attribute of BGP route is set.
Set the community attributes of BGP route	<b>set communitiy</b> { <i>community-number</i>   <b>additive</b>   <b>local-AS</b>   <b>internet</b>   <b>no-advertise</b>   <b>no-export</b>   <b>none</b> }	Optional By default, no community attribute of BGP route is set.
Delete the specified BGP community-list	<b>set comm-list</b> { <i>community-list-number</i> / <i>community-list-name</i> } <b>delete</b>	Optional By default, the BGP community-list is not deleted.
Set BGP route dampening parameters	<b>set dampening</b> <i>half-life start-reusing start-suppress max-duration</i>	Optional By default, no BGP route dampening parameter is set.
Set the extcommunity attributes of MPLS L3VPN route	<b>set extcommunity</b> { <b>rt</b>   <b>soo</b> } <i>extcommunity</i>	Optional By default, no extcommunity attribute

Step	Command	Description
		of MPLS L3VPN route is set.
Set the backup next hop	<b>set fast-reroute</b> [ <b>backup-interface</b> <i>interface-names</i> ] <b>backup-nexthop</b> <i>nexthop-address</i>	Optional By default, the backup next hop of route is not configured.
Set the next hop of route	<b>set ip default next-hop</b> <i>ip-address</i>	Optional By default, the next hop of route is not configured. Set the next hop of route in the redistribution of OSPF route
Set the next hop of route	<b>set ip next-hop</b> <i>ip-address</i>	Optional By default, the next hop of route is not configured. Set the next hop of route for BGP's associated routing map
Set preference of BGP route	<b>set local-preference</b> <i>value</i>	Optional By default, no local preference of BGP route is set.
Set the metric value of route	<b>set metric</b> { <i>metric</i>   <i>+metric</i>   <i>-metric</i>   <i>bandwidth delay reliable loading mtu</i> }	Optional By default, no metric value of route is set.
Set the metric type of route	<b>set metric-type</b> { <b>external</b>   <b>internal</b>   <b>type-1</b>   <b>type-2</b> }	Optional By default, no metric type of route is set.

Step	Command	Description
Set the Origin attributes of BGP route	<b>set origin</b> { <b>egp</b> <i>as-number</i>   <b>igp</b>   <b>incomplete</b> }	Optional By default, no Origin attribute of BGP route is set.
Set the field of external route's tag option	<b>set tag</b> <i>tag-value</i>	Optional By default, no field of external route's tag option is set.
Set the weight of BGP route	<b>set weight</b> <i>weight-value</i>	Optional By default, the weight of BGP route is not set.

## 63.2.6 Configure Key-chain

### Configuration Condition

None

### Configure Key-chain

Key-chain is a password management tool. It provides authentication password when the routing protocol is authenticating protocol packets. Key-chain can provide different passwords for the sending and receiving of packets as well as for different Key IDs. Besides, Key-chain can periodically and automatically switch password according to the effective time of the Key configured, i.e. use different passwords at different time periods, which greatly improves the security of password.

Multiple Key IDs can be configured for a Key-chain. When the protocol uses the Key-chain for authentication, the Key ID is selected according to the following rules:

- Obtain the minimum valid sending password of Key ID when necessary;
- Obtain the minimum valid receiving password of Key ID in the Key where the Key ID is greater than or equals to the given Key ID;
- When the protocol packets received contain Key ID, they will search corresponding valid receiving password in the local port according to this Key ID; otherwise, the minimum valid effective receiving password of the Key ID in the Key-chain of local port will be used.

Table 63 Configuring Key-chain

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure to generate a Key-chain	<b>key chain</b> <i>keychain-name</i>	Mandatory By default, Key-chain is not configured.
Configure Key ID	<b>key</b> <i>key-id</i>	Mandatory By default, Key ID is not configured.
Configure password	<b>key-string</b> [ <b>0</b>   <b>7</b> ] <i>password</i>	Mandatory By default, password is not configured. Please note that space is also considered as a password character
Set the valid time of Key as a receiving password	<b>accept-lifetime</b> <i>time-start</i> { <i>time-end</i>   <b>duration</b> <i>second</i>   <b>infinite</b> }	Mandatory By default, the receiving password is always valid.
Set the valid time of Key as a sending password	<b>send-lifetime</b> <i>time-start</i> { <i>time-end</i>   <b>duration</b> <i>second</i>   <b>infinite</b> }	Mandatory By default, the sending password is always valid.

## 63.2.7 Routing policy tool monitoring and maintaining

Table 63 Routing Policy Tool Monitoring and Maintaining

Command	Description
<b>clear ip prefix-list</b> [ <i>prefix-list-name</i> <i>network/length</i> ]	Clears prefix list statistics.
<b>show ip prefix-list</b> [ <i>prefix-list-name</i> [ <i>network/length</i> [ <b>first-match</b>   <b>longer</b> ]   <b>seq sep_value</b> ]   <b>detail</b> [ <i>prefix-list-name</i> ]   <b>orf-prefix</b>   <b>summary</b> [ <i>prefix-list-name</i> ]	Show the information of prefix list
<b>show ip as-path-access-list</b> [ <i>list-name</i> ]	Show the information of AS-PATH list
<b>show ip community-list</b> [ <i>community-list-number</i>   <i>community-list-name</i> ]	Show the information of community-list
<b>show ip extcommunity-list</b> [ <i>extcommunity-list-number</i>   <i>extcommunity-list-name</i> ]	Show the information of extcommunity-list
<b>show route-map</b> [ <i>route-map-name</i> ]	Show the information of routing map
<b>show key chain</b> [ <i>keychain-name</i> ]	Show the information of Key-chain

## 63.3 Example of typical routing policy tool configuration

### 63.3.1 Configure route redistribution and associate routing policy

#### Network Requirements

- OSPF protocol is run between Device1 and Device2, and RIP protocol is run between Device2 and Device3.
- Configure OSPF to redistribute RIP routes on Device2, associate the routing policy, modify the Tag attribute of 100.1.1.0/24 as 5 and the metric value of 110.1.1.0/24 as 50, and keep the attributes of 120.1.1.0/24 unchanged.

#### Network Topology

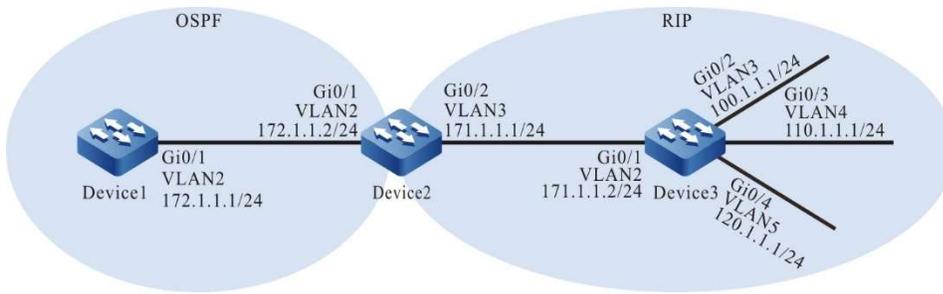


Figure 63-1 Network Topology for Configuring Route Redistribution and Association with Routing Policy

### Configuration Steps

- Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)
- Step 2: Configure IP addresses for the ports. (Omitted)
- Step 3: Configure OSPF.

#### #Configure Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#network 172.1.1.0 0.0.0.255 area 0
Device1(config-ospf)#exit
```

#### #Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 172.1.1.0 0.0.0.255 area 0
Device2(config-ospf)#exit
```

#### Step 4: Configure RIP.

#### #Configure Device2.

```
Device2(config)#router rip
Device2(config-rip)#version 2
Device2(config-rip)#network 171.1.1.0
Device2(config-rip)#exit
```

#### #Configure Device3.

```
Device3(config)#configure terminal
Device3(config)#router rip
Device3(config-rip)#version 2
Device3(config-rip)#network 171.1.1.0
Device3(config-rip)#network 100.1.1.0
Device3(config-rip)#network 110.1.1.0
Device3(config-rip)#network 120.1.1.0
Device3(config-rip)#exit
```

Step 5: Configure OSPF to redistribute RIP routes.

#Configure Device2.

```
Device2(config)#router ospf 100
Device2(config-ospf)#redistribute rip
Device2(config-ospf)#exit
```

#View the routing table of Device1.

```
Device1#show ip route ospf
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

OE 100.1.1.0/24 [150/20] via 172.1.1.2, 02:22:08, vlan2
OE 110.1.1.0/24 [150/20] via 172.1.1.2, 00:49:57, vlan2
OE 120.1.1.0/24 [150/20] via 172.1.1.2, 02:22:08, vlan2
OE 171.1.1.0/24 [150/20] via 172.1.1.2, 02:22:41, vlan2
```

By checking the routing table of Device1, you will find that the RIP routes on Device2, i.e. 100.1.1.0/24, 110.1.1.0/24, and 120.1.1.0/24, have been redistributed to the OSPF process and successfully advertised to Device1.

Step 6: Configure access list and routing policy.

#Configure Device2.

Configure access list, and allow the routes 100.1.1.0/24, 110.1.1.0/24 and 120.1.1.0/24 to pass.

```
Device2(config)#ip access-list standard 1
Device2(config-std-nacl)#permit 100.1.1.0 0.0.0.255
Device2(config-std-nacl)#commit
Device2(config-std-nacl)#exit
Device2(config)#ip access-list standard 2
Device2(config-std-nacl)#permit 110.1.1.0 0.0.0.255
Device2(config-std-nacl)#commit
Device2(config-std-nacl)#exit
Device2(config)#ip access-list standard 3
Device2(config-std-nacl)#permit 120.1.1.0 0.0.0.255
Device2(config-std-nacl)#commit
Device2(config-std-nacl)#exit
```

Configure the routing policy rip\_to\_ospf. Set the tag attribute of the routes allowed by the access list with a match number of 1, set the metric attribute of the routes allowed by the access list with a match number of 2, and keep the attributes of the routes allowed by the access list with a match number of 3 unchanged.

```
Device2(config)#route-map rip_to_ospf 10
Device2(config-route-map)#match ip address 1
Device2(config-route-map)#set tag 5
Device2(config-route-map)#exit
Device2(config)#route-map rip_to_ospf 20
Device2(config-route-map)#match ip address 2
Device2(config-route-map)#set metric 50
```

```
Device2(config-route-map)#exit
Device2(config)#route-map rip_to_ospf 30
Device2(config-route-map)#match ip address 3
Device2(config-route-map)#exit
```

---

## Note

- When configuring a routing policy, both the prefix list and ACL can create matching rules. The difference is that the prefix list can exactly match the routing mask.
- 

Step 7: Configure OSPF to redistribute RIP routes and associate routing policy.

#Configure Device2.

```
Device2(config)#router ospf 100
Device2(config-ospf)#redistribute rip route-map rip_to_ospf
Device2(config-ospf)#exit
```

Step 8: Check the result.

#View the OSPF database of Device1.

```
Device1#show ip ospf database external
      OSPF Router with ID (172.1.1.1) (Process ID 100)

      AS External Link States

      LS age: 1183
      Options: 0x22 (-|-|DC|-|-|E|-)
      LS Type: AS-external-LSA
      Link State ID: 100.1.1.0 (External Network Number)
      Advertising Router: 172.1.1.2
      LS Seq Number: 80000006
      Checksum: 0xbcc0
      Length: 36
      Network Mask: /24
        Metric Type: 2 (Larger than any link state path)
        TOS: 0
        Metric: 20
        Forward Address: 0.0.0.0
        External Route Tag: 5

      LS age: 1233
      Options: 0x22 (-|-|DC|-|-|E|-)
      LS Type: AS-external-LSA
      Link State ID: 110.1.1.0 (External Network Number)
      Advertising Router: 172.1.1.2
      LS Seq Number: 80000006
```

Checksum: 0x0d4d  
Length: 36  
Network Mask: /24  
Metric Type: 2 (Larger than any link state path)  
TOS: 0  
Metric: 50  
Forward Address: 0.0.0.0  
External Route Tag: 0

LS age: 1113  
Options: 0x22 (-|DC|-|E|-)  
LS Type: AS-external-LSA  
Link State ID: 120.1.1.0 (External Network Number)  
Advertising Router: 172.1.1.2  
LS Seq Number: 80000005  
Checksum: 0x5f10  
Length: 36  
Network Mask: /24  
Metric Type: 2 (Larger than any link state path)  
TOS: 0  
Metric: 20  
Forward Address: 0.0.0.0  
External Route Tag: 0

### #View the routing table of Device1.

```
Device1#show ip route ospf
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

OE 100.1.1.0/24 [150/20] via 172.1.1.2, 02:30:28, vlan2
OE 110.1.1.0/24 [150/50] via 172.1.1.2, 00:58:17, vlan2
OE 120.1.1.0/24 [150/20] via 172.1.1.2, 02:30:28, vlan2
```

By checking the OSPF database and routing table of Device1, you will find that the route tag of 100.1.1.0/24 is 5, the metric value of 110.1.1.0/24 is 50, and the route attributes of 120.1.1.0/24 remain the same.

---

## Note

- When external routes are redistributed, the direct routes covered by the RIP process will also be redistributed into the target protocol.
- 

## 63.3.2 Configure BGP to associate with the routing policy

### Network Requirements

- Device1 runs IGP protocol OSPF with Device2 and Device3 to establish IBGP neighbors, and Device4 establishes EBGP neighbors with Device2 and Device3.

- Routing policy is required to be configured on Device2 and Device3. In this case, some data of Device1 will reach the network segment 100.1.1.0/24 through Device2 and some reach the network segment 110.1.1.0/24 through Device3; some data of Device4 will reach the network segment 120.1.1.0/24 through Device2 and some reach the network segment 130.1.1.0/24 through Device3.

### Network Topology

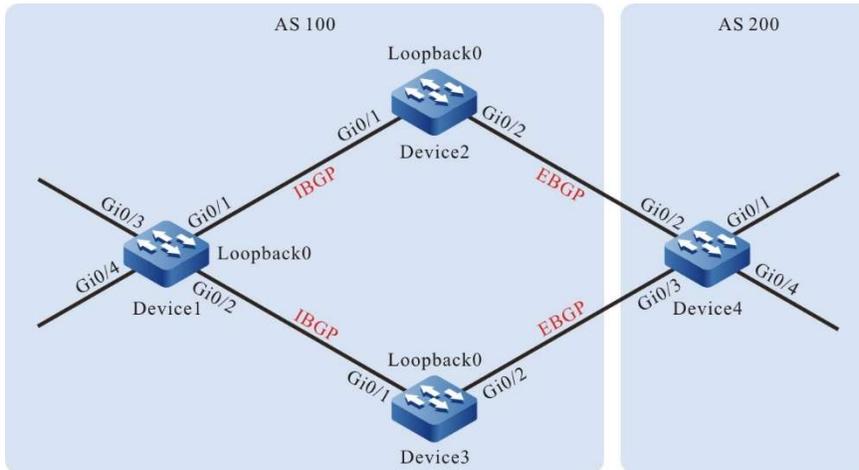


Figure 63-2 Network Topology for Configuring BGP Association with Routing Policy

of equipment	Interface	VLAN	IP address
Device1	Gi0/1	2	1.0.0.1/24
	Gi0/2	3	2.0.0.1/24
	Gi0/3	4	120.1.1.1/24
	Gi0/4	5	130.1.1.1/24
	Loopback0		38.1.1.1/32
Device2	Gi0/1	2	1.0.0.2/24
	Gi0/2	3	3.0.0.1/24
	Loopback0		39.1.1.1/32
Device3	Gi0/1	2	2.0.0.2/24

of equipment	Interface	VLAN	IP address
	Gi0/2	3	4.0.0.1/24
	Loopback0		40.1.1.1/32
Device4	Gi0/1	2	100.1.1.1/24
	Gi0/2	3	3.0.0.2/24
	Gi0/3	4	4.0.0.2/24
	Gi0/4	5	110.1.1.1/24

## Configuration Steps

- Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)
- Step 2: Configure IP addresses for the ports. (Omitted)
- Step 3: Configure OSPF so that the routes of Loopback between devices are reachable from each other.

### #Configure Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#network 1.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 38.1.1.1 0.0.0.0 area 0
Device1(config-ospf)#exit
```

### #Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 1.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#network 39.1.1.1 0.0.0.0 area 0
Device2(config-ospf)#exit
```

### #Configure Device3.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 40.1.1.1 0.0.0.0 area 0
Device3(config-ospf)#exit
```

### #View the routing table of Device1.

```
Device1#show ip route ospf
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

O 39.1.1.1/32 [110/2] via 1.0.0.2, 19:11:33, vlan2
O 40.1.1.1/32 [110/2] via 2.0.0.2, 18:56:32, vlan3
```

### #View the routing table of Device 2.

```
Device2#show ip route ospf
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

O 2.0.0.0/24 [110/2] via 1.0.0.1, 19:19:10, vlan2
O 38.1.1.1/32 [110/2] via 1.0.0.1, 19:09:43, vlan2
O 40.1.1.1/32 [110/3] via 1.0.0.1, 18:56:49, vlan2
```

### #Check the routing table of Device3.

```
Device3#show ip route ospf
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

O 1.0.0.0/24 [110/2] via 2.0.0.1, 19:17:33, vlan2
O 38.1.1.1/32 [110/2] via 2.0.0.1, 19:09:59, vlan2
O 39.1.1.1/32 [110/3] via 2.0.0.1, 19:12:06, vlan2
```

After the configuration, Device1 establishes OSPF neighbors with Device2 and Device3, and learn the Loopback route from each other.

#### Step 4: Configure BGP.

### #Configure Device1.

Configure Device1 to establish IBGP neighbors with Device2 and Device3 using Loopback interface address, and advertise the routes 120.1.1.0/24 and 130.1.1.0/24 to the BGP routing table.

```
Device1(config)#router bgp 100
Device1(config-bgp)#neighbor 39.1.1.1 remote-as 100
Device1(config-bgp)#neighbor 39.1.1.1 update-source loopback0
Device1(config-bgp)#neighbor 40.1.1.1 remote-as 100
Device1(config-bgp)#neighbor 40.1.1.1 update-source loopback0
Device1(config-bgp)#network 120.1.1.0 255.255.255.0
Device1(config-bgp)#network 130.1.1.0 255.255.255.0
Device1(config-bgp)#exit
```

### #Configure Device2.

```
Device2(config)#router bgp 100
Device2(config-bgp)#neighbor 38.1.1.1 remote-as 100
Device2(config-bgp)#neighbor 38.1.1.1 update-source loopback0
Device2(config-bgp)#neighbor 38.1.1.1 next-hop-self
Device2(config-bgp)#neighbor 3.0.0.2 remote-as 200
Device2(config-bgp)#exit
```

### #Configure Device3.

```
Device3(config)#router bgp 100
Device3(config-bgp)#neighbor 38.1.1.1 remote-as 100
Device3(config-bgp)#neighbor 38.1.1.1 update-source loopback0
Device3(config-bgp)#neighbor 38.1.1.1 next-hop-self
Device3(config-bgp)#neighbor 4.0.0.2 remote-as 200
Device3(config-bgp)#exit
```

### #Configure Device4.

Configure Device4 to establish EBGP neighbors with Device2 and Device3, and advertise the routes 100.1.1.0/24 and 110.1.1.0/24 to the BGP routing table.

```
Device4#configure terminal
Device4(config)#router bgp 200
Device4(config-bgp)#neighbor 3.0.0.1 remote-as 100
Device4(config-bgp)#neighbor 4.0.0.1 remote-as 100
Device4(config-bgp)#network 100.1.1.0 255.255.255.0
Device4(config-bgp)#network 110.1.1.0 255.255.255.0
Device4(config-bgp)#exit
```

### #View the BGP routing information of Device1.

```
Device1#show ip bgp
BGP table version is 2, local router ID is 38.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop        Metric LocPrf Weight Path
  [B]*>i100.1.1.0/24  39.1.1.1         0  100   0 200 i
  [B]* i           40.1.1.1         0  100   0 200 i
  [B]*>i110.1.1.0/24  39.1.1.1         0  100   0 200 i
  [B]* i           40.1.1.1         0  100   0 200 i
  [B]*> 120.1.1.0/24  0.0.0.0          0   32768 i
  [B]*> 130.1.1.0/24  0.0.0.0          0   32768 i
```

### #View the routing table of Device1.

```
Device1#show ip route bgp
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

B 100.1.1.0/24 [200/0] via 39.1.1.1, 19:03:19, vlan2
B 110.1.1.0/24 [200/0] via 39.1.1.1, 19:03:19, vlan2
```

It can be seen from the BGP routing table of Device1 that there are two valid routes for the data leading to the network segments 100.1.1.0/24 and 110.1.1.0/24. Since the router ID of Device2 is small, the data BGPs all reach the network segments 100.1.1.0/24 and 110.1.1.0/24 through Device2 by default.

### #View the BGP routing information of Device 4.

```
Device4#show ip bgp
BGP table version is 3, local router ID is 110.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop        Metric LocPrf Weight Path
  [B]*> 100.1.1.0/24  0.0.0.0          0   32768 i
  [B]*> 110.1.1.0/24  0.0.0.0          0   32768 i
```

```

[B]* 120.1.1.0/24 4.0.0.1 0 0 100 i
[B]*> 3.0.0.1 0 0 100 i
[B]* 130.1.1.0/24 4.0.0.1 0 0 100 i
[B]*> 3.0.0.1 0 0 100 i

```

#### #View the routing table of Device 4.

```

Device4#show ip route bgp
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

B 120.1.1.0/24 [20/0] via 3.0.0.1, 19:25:05, vlan3
B 130.1.1.0/24 [20/0] via 3.0.0.1, 19:25:05, vlan3

```

It can be seen from the BGP routing table of Device4 that there are two valid routes for the data leading to the network segments 120.1.1.0/24 and 130.1.1.0/24. Since Device4 first establishes neighbors with Device2 and it takes longer to learn these two routes from Device2, the data BGP's all reach the network segments 120.1.1.0/24 and 130.1.1.0/24 through Device2 by default.

Step 5: Configure prefix list and routing policy.

#### #Configure Device2.

Configure prefix list, and allow the routes 100.1.1.0/24 and 130.1.1.0/24 to pass.

```

Device2(config)#ip prefix-list 1 permit 100.1.1.0/24
Device2(config)#ip prefix-list 2 permit 130.1.1.0/24

```

Configure routing policy Ip so that Device2 sets local-preference attribute for the routes allowed by the prefix list with the match number of 1.

```

Device2(config)#route-map lp 10
Device2(config-route-map)#match ip address prefix-list 1
Device2(config-route-map)#set local-preference 200
Device2(config-route-map)#exit
Device2(config)#route-map lp 20
Device2(config-route-map)#exit

```

Configure the routing policy med so that Device2 sets MED attribute for the routes allowed by the prefix list with the match number of 2.

```

Device2(config)#route-map med 10
Device2(config-route-map)#match ip address prefix-list 2
Device2(config-route-map)#set metric 10
Device2(config-route-map)#exit
Device2(config)#route-map med 20
Device2(config-route-map)#exit

```

#### #Configure Device3.

Configure prefix list, and allow the routes 110.1.1.0/24 and 120.1.1.0/24 to pass.

```

Device3(config)#ip prefix-list 1 permit 110.1.1.0/24
Device3(config)#ip prefix-list 2 permit 120.1.1.0/24

```

Configure routing policy Ip so that Device3 sets local-preference attribute for the routes allowed by the prefix list with the match number of 1.

```
Device3(config)#route-map lp 10
Device3(config-route-map)#match ip address prefix-list 1
Device3(config-route-map)#set local-preference 200
Device3(config-route-map)#exit
Device3(config)#route-map lp 20
Device3(config-route-map)#exit
```

Configure the routing policy med so that Device3 sets MED attribute for the routes allowed by the prefix list with the match number of 2.

```
Device3(config)#route-map med 10
Device3(config-route-map)# match ip address prefix-list 2
Device3(config-route-map)#set metric 10
Device3(config-route-map)#exit
Device3(config)#route-map med 20
Device3(config-route-map)#exit
```

---

 **Note**

- When configuring a routing policy, both the prefix list and ACL can create matching rules. The difference is that the prefix list can exactly match the routing mask.
- 

Step 6: Configure BGP to associate with the routing policy.

#Configure Device2.

Apply the routing policy lp to the routes of neighbor 38.1.1.1 in the outgoing direction and med to those of neighbor 3.0.0.2 in the outgoing direction.

```
Device2(config)#router bgp 100
Device2(config-bgp)#neighbor 38.1.1.1 route-map lp out
Device2(config-bgp)#neighbor 3.0.0.2 route-map med out
Device2(config-bgp)#exit
```

#Configure Device3.

Apply the routing policy lp to the routes of neighbor 38.1.1.1 in the outgoing direction and med to those of neighbor 4.0.0.2 in the outgoing direction.

```
Device3(config)#router bgp 100
Device3(config-bgp)#neighbor 38.1.1.1 route-map lp out
Device3(config-bgp)#neighbor 4.0.0.2 route-map med out
Device3(config-bgp)#exit
```

Step 7: Check the result.

#View the BGP routing information of Device1.

```

Device1#show ip bgp
BGP table version is 9, local router ID is 38.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop        Metric LocPrf Weight Path
[B]* i100.1.1.0/24  40.1.1.1         0 100  0 200 i
[B]*>i             39.1.1.1         0 200  0 200 i
[B]*>i110.1.1.0/24  40.1.1.1         0 200  0 200 i
[B]* i             39.1.1.1         0 100  0 200 i
[B]*> 120.1.1.0/24  0.0.0.0          0 32768 i
[B]*> 130.1.1.0/24  0.0.0.0          0 32768 i

```

#### #View the routing table of Device1.

```

Device1#show ip route bgp
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

B 100.1.1.0/24 [200/0] via 39.1.1.1, 02:58:12, vlan2
B 110.1.1.0/24 [200/0] via 40.1.1.1, 02:58:10, vlan3

```

It can be seen from the BGP routing table of Device1 that the route 100.1.1.0/24 has two next hops, i.e. 40.1.1.1 and 39.1.1.1. The local preference of the route with the next hop of 39.1.1.1 becomes 200, so the data prefer to reach the network segment 100.1.1.0/24 through Device2. There are also two next hops on the route 110.1.1.0/24, i.e. 40.1.1.1 and 39.1.1.1. The local preference of the route with the next hop of 40.1.1.1 becomes 200, so the data prefer to reach the network segment 110.1.1.0/24 through Device3.

#### #View the BGP routing information of Device 4.

```

Device4#show ip bgp
BGP table version is 9, local router ID is 110.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop        Metric LocPrf Weight Path
[B]*> 100.1.1.0/24  0.0.0.0          0 32768 i
[B]*> 110.1.1.0/24  0.0.0.0          0 32768 i
[B]* 120.1.1.0/24   4.0.0.1          10 0 100 i
[B]*>             3.0.0.1          0 0 100 i
[B]*> 130.1.1.0/24  4.0.0.1          0 0 100 i
[B]*             3.0.0.1          10 0 100 i

```

#### #View the routing table of Device 4.

```

Device4#show ip route bgp
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

B 120.1.1.0/24 [20/0] via 3.0.0.1, 03:05:39, vlan3
B 130.1.1.0/24 [20/0] via 4.0.0.1, 03:05:37, vlan4

```

It can be seen from the BGP routing table of Device1 that the route 120.1.1.0/24 has two next hops, i.e. 4.0.0.1 and 3.0.0.1. The metric of the route with the next hop of 4.0.0.1 becomes 10, so the data prefer to reach the network segment 120.1.1.0/24 through Device2. There are also two next hops on the route 130.1.1.0/24, i.e. 4.0.0.1 and 3.0.0.1. The metric of the route with the next hop of 3.0.0.1 becomes 10, so the data prefer to reach the network segment 130.1.1.0/24 through Device3.

---

**Note**

- When BGP peer or peer group applies the routing policy, it can be used in the receiving and advertising direction of the peer or peer group. This takes effect after resetting BGP.
- 

# 64 L2 Multicast Basics

---

## 64.1 Overview

The main task of L2 multicast basics is to maintain the L2 multicast forwarding table. The application modules of L2 multicast generates their L2 multicast tables by static configuration and dynamic learning, and then synchronize the information to the L2 multicast basis modules. L2 multicast basis modules integrate the information to form the L2 multicast forwarding table.

## 64.2 L2 Multicast Basics Function Configuration

Table 64-1 L2 Multicast Basics Configuration List

Configuration Task	
Configure Unknown Packet Forwarding Policy of L2 Multicast	Configure Unknown Packet MAC Forwarding Policy of L2 Multicast

Configuration Task	
Configure L2 static multicast	Configure L2 static multicast

### 64.2.1 Configure Unknown Packet Forwarding Policy of L2 Multicast

Unknown multicast service packets have two kinds of forwarding policies: drop unknown multicast service packets, or make the unknown multicast service packets flood.

#### Configuration Condition

Before configuring the unknown packet forwarding policy of L2 multicast, first complete the following task:

- Configure corresponding VLAN

#### Configure Unknown Packet MAC Forwarding Policy of L2 Multicast

In the L2 multicast MAC forwarding mode, the multicast service packets are forwarded by matching VLAN and destination MAC address. When the multicast service packet does not match the forwarding table, it is unknown multicast service packet. The device has two kinds of forwarding policies for the unknown multicast service packets: drop unknown multicast service packets, or make unknown multicast service packets flood.

Table 64-2 Configuring Unknown Packet MAC Forwarding Policy of L2 Multicast

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the VLAN configuration mode	<b>vlan <i>vlan-id</i></b>	-
Configure the forwarding policy of L2 multicast	<b>l2-multicast drop-unknown</b>	Optional By default, the function of dropping unknown multicast service packets is disabled in the VLAN

#### Configure Unknown Packet IP Forwarding Policy of L2 Multicast

In the IPV4 L2 multicast IP forwarding mode, the multicast service packets are forwarded by matching VLAN, multicast source IP address and multicast destination IP address. When the multicast service packet does not match the forwarding table, it is unknown multicast service packet. The device has two kinds of forwarding policies for the unknown multicast service packets: drop unknown multicast service packets, or make unknown multicast service packets flood.

Table 64-3 Configuring Unknown Packet IP Forwarding Policy of L2 Multicast

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the VLAN configuration mode	<b>vlan <i>vlan-id</i></b>	-
Configure the IP forwarding policy of L2 multicast	<b>I3-multicast drop-unknown</b>	Mandatory By default, the function of dropping unknown multicast service packets is disabled in the VLAN

### Configure Unknown Packet Ipv6 Forwarding Policy of L2 Multicast

In the IPV6 L2 multicast IP forwarding mode, the multicast service packets are forwarded by matching VLAN, multicast source IP address and multicast destination IP address. When the multicast service packet does not match the forwarding table, it is unknown multicast service packet. The device has two kinds of forwarding policies for the unknown multicast service packets: drop unknown multicast service packets, or make unknown multicast service packets flood.

Table 64-4 Configuring Unknown Packet IPv6 Forwarding Policy of L2 Multicast

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the VLAN configuration mode	<b>vlan <i>vlan-id</i></b>	-
Configure the IP forwarding policy of L2 multicast	<b>I3-multicast ipv6 drop-unknown</b>	Mandatory By default, the function of dropping unknown

Step	Command	Description
		multicast service packets is disabled in the VLAN

### Configure Policy of Forwarding Unknown Multicast to Uplink Port

In the L2 multicast forwarding, the multicast service packets are forwarded by the L2 multicast forwarding table. When the multicast service packet does not match the forwarding table, it is unknown multicast service packet. The function of dropping unknown multicast service packets is enabled in the VLAN, and the unknown multicast service packets will be dropped. In this case, after the function of forwarding unknown multicast to the uplink port is enabled in the VLAN, the effect of flooding the unknown multicast service packets to the uplink port can be realized.

Table 64-5 Configuring the Policy of Forwarding Unknown Multicast to Uplink Port

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the VLAN configuration mode	<b>vlan <i>vlan-id</i></b>	-
Configure the IP forwarding policy of L2 multicast	<b>l3-multicast drop-unknown</b>	Mandatory By default, the function of dropping unknown multicast service packets is disabled in the VLAN
Configure the MAC forwarding policy of L2 multicast	<b>l2-multicast drop-unknown</b>	Mandatory By default, the function of dropping unknown multicast service packets is disabled in the VLAN
Configure Policy of Forwarding Unknown Multicast to Uplink Port	<b>multicast mrouter-forwarding</b>	Optional By default, forwarding the unknown multicast to the uplink port is not enabled in the VLAN

## 64.2.2 Configure L2 static multicast

L2 static multicast generates L2 multicast forwarding table by static configuration. It is formed by the user specifying multicast MAC address, VLAN, and port list (including member port list and prohibited port list).

### Configuration Condition

Before configuring L2 static multicast, first complete the following task:

- Configure corresponding VLAN

### Configure L2 static multicast

Table 64-6 Configuring L2 Static Multicast

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Create L2 static multicast	<b>l2-multicast mac-entry static mac-address vlan vlan-id</b>	Mandatory By default, no L2 static multicast entry is configured
Configure the member port for L2 static multicast entries	<b>interface interface-list-name { member   forbidden }</b>	Optional By default, the member port for L2 static multicast entries is not configured
Configure the member aggregation group for L2 static multicast entries	<b>interface link-aggregation link-aggregation-id { member   forbidden }</b>	Optional The member aggregation group for L2 static multicast entries is not configured

## 64.2.3 Monitoring and Maintaining of L2 Multicast Basics

Table 64-7 Monitoring and Maintaining of L2 Multicast Basics

Command	Description
<b>show l2-multicast ha { phase batch   phase flat   statistics }</b>	Show the information about high reliability of the L2 multicast
<b>show l2-multicast ip-entry</b>	Show the information of the IP forwarding table of the L2 multicast
<b>show l2-multicast l3-ip-entry</b>	Show the information of the L3 IP forwarding table of the L2 multicast
<b>show l2-multicast mac-entry { all   forward   static }</b>	Show the L2 multicast table
<b>show l2-multicast vlan-setting { all   vlan-id }</b>	Show the VLAN information of the L2 multicast

## 64.3 Typical Configuration Examples of L2 Static Multicast

### 64.3.1 Configure L2 static multicast

#### Network Requirements

- On Device 1, configure the multicast routing protocol, on Device 2, configure the L2 static multicast in VLAN 2, PC1 is the receiver of multicast services, and PC2 and PC3 are not receivers of multicast services.
- Multicast Server sends the multicast service packets, PC 1 can correctly receive the multicast service packets, and PC 2 and PC 3 cannot receive the multicast service packets.

#### Network Topology

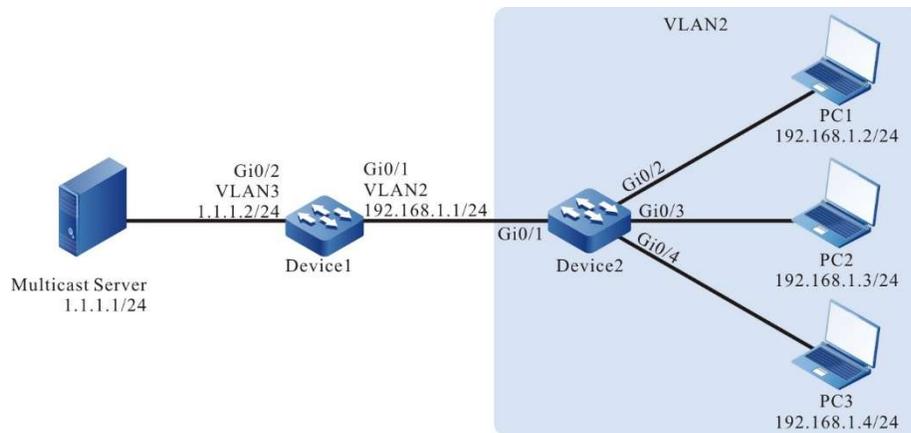


Figure 64-1 Network Topology for Configuring L2 Static Multicast

### Configuration Steps

Step 1: On Device 1, configure the interface IP address and enable the multicast routing protocol. (Omitted)

Step 2: Configure Device2.

Create VLAN2 on #Device 2.

```
Device2#configure terminal
Device2(config)#vlan 2
Device2(config-vlan2)#exit
```

#On Device 2, configure the link type of ports gigabitethernet0/2-gigabitethernet0/4 to Access to allow services of VLAN 2 to pass.

```
Device2(config)#interface gigabitethernet 0/2-0/4
Device2(config-if-range)#switchport access vlan 2
Device2(config-if-range)#exit
```

#On Device 2, configure the link type of port gigabitethernet0/1 to Trunk to allow services of VLAN 2 to pass, and configure PVID to 1.

```
Device2(config)#interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#switchport mode trunk
Device2(config-if-gigabitethernet0/1)#switchport trunk allowed vlan add 2
Device2(config-if-gigabitethernet0/1)#switchport trunk pvid vlan 1
Device2(config-if-gigabitethernet0/1)#exit
```

#Enable unknown multicast drop in VLAN 2.

```
Device2(config)#vlan 2
Device2(config-vlan2)#l2-multicast drop-unknown
```

```
Device2(config-vlan2)#exit
```

### #Configure L2 static multicast group members.

```
Device2(config)#l2-multicast mac-entry static 0100.5E01.0101 vlan 2
```

```
Device2(config-mcast)#interface gigabitethernet 0/2 member
```

```
Device2(config-mcast)#exit
```

```
Device2(config)#l2-multicast mac-entry static 0100.5E01.0101 vlan 2
```

```
Device2(config-mcast)#interface gigabitethernet 0/3 forbidden
```

```
Device2(config-mcast)#exit
```

### Step 3: Check the result.

### #View the L2 static multicast entries of Device 2.

```
Device2#show l2-multicast mac-entry static
```

```
Current L2 Static Multicast 1 entries
```

```
-----  
NO.  VID   Group MAC address  Interface Name  
-----  
1    2      0100.5E01.0101    [M] gi0/2  
                               [F] gi0/3
```

#Multicast Server sends the multicast service packet with the destination address of 224.1.1.1, PC1 can correctly receive the multicast service packet, and PC2 and PC3 cannot receive the multicast service packet.

## 64.3.2 Configure IPv6 L2 Static Multicast

### Network Requirements

- On Device 1, configure the IPv6 multicast routing protocol, on Device 2, configure the IPv6 L2 static multicast in VLAN 2, PC1 is the receiver of multicast services, and PC2 and PC3 are receivers of non-multicast services;
- Multicast Server sends the IPv6 multicast service packets, PC1 can correctly receive the multicast service packets, and PC2 and PC3 cannot receive the multicast service packets.

### Network Topology

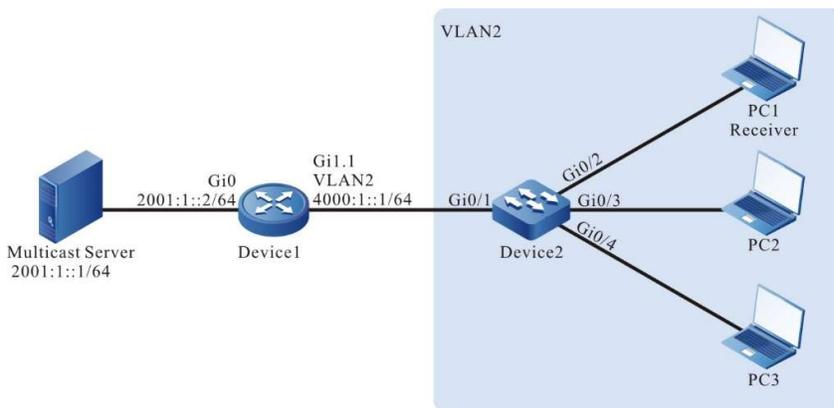


Figure 64-2 Network Topology for Configuring IPv6 L2 Static Multicast

### Configuration Steps

Step 1: On Device 1, configure the interface IP address and enable the multicast routing protocol.  
(Omitted)

Step 2: Configure Device2.

Create VLAN2 on #Device 2.

```
Device2#configure terminal
Device2(config)#vlan 2
Device2(config-vlan2)#exit
```

#On Device 2, configure the link type of ports gigabitethernet0/2-gigabitethernet0/4 to Access to allow services of VLAN 2 to pass.

```
Device2(config)#interface gigabitethernet 0/2-0/4
Device2(config-if-range)#switchport access vlan 2
Device2(config-if-range)#exit
```

#On Device 2, configure the link type of port gigabitethernet0/1 to Trunk to allow services of VLAN 2 to pass, and configure PVID to 1.

```
Device2(config)#interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#switchport mode trunk
Device2(config-if-gigabitethernet0/1)#switchport trunk allowed vlan add 2
Device2(config-if-gigabitethernet0/1)#switchport trunk pvid vlan 1
Device2(config-if-gigabitethernet0/1)#exit
```

#Enable unknown multicast drop in VLAN 2.

```
Device2(config)#vlan 2
Device2(config-vlan2)#l2-multicast drop-unknown
Device2(config-vlan2)#exit
```

#Configure L2 static multicast group members.

```
Device2(config)# l2-multicast mac-entry static 3333.0000.0001 vlan 2
Device2(config-mcast)#interface gigabitethernet 0/2 member
Device2(config-mcast)#interface gigabitethernet 0/3 forbidden
Device2(config-mcast)#exit
```

Step 3: Check the result.

#View the IPv6 L2 static multicast entries of Device 2.

```
Device2# show l2-multicast mac-entry static
Current L2 Static Multicast 1 entries

-----
NO.  VID   Group MAC address  Interface Name
-----
1   2     3333.0000.0001  [M] gi0/2
                        [F] gi0/3
```

#Multicast Server sends the multicast service packet with the destination address of ff10 ::1, PC 1 can correctly receive the multicast service packet, and PC 2 and PC 3 cannot receive the multicast service packet.

---

## Note

- In the IPv6 L2 static multicast, the multicast service packets are only forwarded to the port whose role is member.
  - For the forbidden port, even if you add the multicast groups corresponding to the static multicast groups by means of mld snooping, the multicast service packet whose destination
-

---

address is the static multicast group will not be forwarded to the forbidden port.

- For the non-member and non-forbidden port, the multicast groups corresponding to the static multicast groups can be added by means of mld snooping, the multicast service packet whose destination address is the static multicast group will be forwarded to such port.
-

# 65 IGMP snooping

## 65.1 Overview

IGMP Snooping (Internet Group Management Protocol snooping) is the function designed for the device that does not support IGMP to reduce the spreading range of the multicast service packet and prevent the multicast packet from being spread to the network segments that do not need the multicast packet. It forms and maintains the downstream member port list of each multicast group at the local by listening to IGMP packets. In this way, when receiving multicast service packet, forward at the specified downstream member port. Meanwhile, IGMP Snooping can listen to the IGMP protocol packets and cooperate with the upstream multicast router to manage and control multicast services.

IGMP Snooping mainly realizes the following functions:

- Listen to the IGMP packets to set up multicast information. IGMP Snooping gets the downstream multicast receiver information by listening to IGMP packets, realizing the forwarding of multicast service packets at the specified member port.
- Listen to the IGMP protocol packets. In this way, the upstream multicast router can correctly maintain IGMP member relation table.

## 65.2 IGMP snooping Function Configuration

Table 65-1 IGMP Snooping Function Configuration List

Configuration Task	
Configure the basic functions of IGMP snooping	Enable the IGMP snooping function
	Configure the IGMP snooping version
	Enable the IGMP snooping L2 forwarding function
Configure IGMP snooping Querier	Enable IGMP snooping Querier
	Configure the source IP address of the IGMP query packet

Configuration Task	
	Configure Query Interval of General Group
	Configure Max. Response Time
	Configure Query Interval of Specified Group
	Configure Fast Leave
Configure IGMP snooping Router Port	Configure IGMP snooping Router Port
	Configure age time for the IGMP snooping dynamic router port
Configure the IGMP snooping TCN event	Enable fast convergence
	Configure TCN event query interval
	Configure TCN event query count
Configure the IGMP snooping policy	Configure the port filtering rules
	Configure the maximum number of port multicast group entries
	Configure the upper limit policy of port multicast groups
Configure IGMP snooping Proxy	Configure IGMP snooping Proxy

### 65.2.1 Configure the basic functions of IGMP snooping

In the various configuration tasks for IGMP snooping, you must first enable the IGMP snooping function so that the configuration of the other function features can take effect.

#### Configuration Condition

Before configuring the basic functions of IGMP snooping, do the following:

- Configure VLAN.

## Enable the IGMP snooping function

The IGMP snooping function will run on the device only after it is enabled.

Table 65-2 Enabling IGMP Snooping Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable the global IGMP snooping function	<b>ip igmp snooping</b>	Mandatory By default, the global IGMP snooping function is disabled
Enable the IGMP snooping function of the specified VLAN	<b>ip igmp snooping vlan <i>vlan-id</i></b>	Mandatory By default, the IGMP snooping function is disabled in the VLAN

---

### Note

- The IGMP snooping function of the specified VLAN can be enabled only after the global IGMP snooping function is enabled.
- 

## Configure the IGMP snooping version

The handling rules for the configured IGMP snooping version and IGMP protocol packets are as follows:

If the configured IGMP snooping version is V3, the device can handle IGMP protocol packets of versions V1, V2, and V3;

If the configured IGMP snooping version is V2, the device can handle IGMP protocol packets of versions V1 and V2, and does not handle the protocol packets of version V3 but floods them in the VLAN;

If the configured IGMP snooping version is V1, the device can handle IGMP protocol packets of version V1, and does not handle the protocol packets of versions V2 and V3 but floods them in the VLAN.

Table 65-3 Configuring IGMP Snooping Version

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the IGMP snooping version	<b>ip igmp snooping vlan <i>vlan-id</i> version <i>version-number</i></b>	Optional By default, the IGMP snooping version is 2

### Enable IGMP Snooping L2 Forwarding

Generally, IGMP snooping forwards the multicast service packets in the VLAN based on the multicast source IP address and the multicast destination IP address. After IGMP snooping L2 forwarding, IGMP snooping will forward the multicast service packets in the VLAN based on the multicast destination MAC address.

Table 65-4 IGMP Snooping L2 Forwarding

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable the L2 multicast L2 forwarding function in the specified VLAN	<b>ip igmp snooping vlan <i>vlan-id</i> l2-forwarding</b>	Mandatory By default, the L2 multicast IP forwarding function of IGMP snooping is enabled for the VLAN

### Caution

- As 32 multicast IP addresses correspond to one multicast MAC address, with L2 forwarding being unable to specify the multicast source forwarding, it is possible that multiple IP multicast source groups correspond to the same MAC group, and then forwarding conflicts may occur.

### 65.2.2 Configure IGMP snooping Querier

If there is no L3 multicast device in the network, it cannot realize the related functions of the IGMP querier. To solve the problem, the IGMP snooping querier can be configured on the L2 multicast device to realize

the IGMP querier function. Therefore, the L2 multicast device can set up and maintain the multicast forwarding entry, so as to forward multicast service packets normally.

### Configuration Condition

Before configuring the basic functions of IGMP snooping querier, first complete the following task:

- Enable global and VLAN IGMP snooping function

### Enable IGMP snooping Querier

You should first enable the IGMP snooping querier function so that the configuration of the other features of the querier can take effect.

Table 65-5 Enabling IGMP snooping Querier

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable IGMP snooping Querier	<b>ip igmp snooping vlan <i>vlan-id</i> querier</b>	Mandatory  By default, the IGMP snooping querier of the specified VLAN is disabled

### Configure Querier IP Address

The querier configured with IP address takes part in the election of the IGMP querier in VLAN and the querier fills the IP address in the source IP address field of the sent IGMP group query packet.

Table 65-6 Configuring Querier IP Address

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure Querier IP Address	<b>ip igmp snooping vlan <i>vlan-id</i> querier address <i>ip-address</i></b>	Mandatory  By default, the querier IP address of the specified VLAN is not configured

---

 **Note**

- When the querier IP address is not configured, the default source IP address of the querier is 0.0.0.0, but the querier does not send the IGMP group query packet with source IP address 0.0.0.0.
- 

### Configure Query Interval of General Group

IGMP querier periodically sends the query packets of the general group to maintain the group member relation. The interval of sending the IGMP general group query packets can be modified according to the actuality of the network. For example, if the configured general group query interval is long, it can reduce the number of the IGMP protocol packets in the network, avoiding the network congestion.

Table 65-7 Configuring Query Interval of General Group

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure Query Interval of General Group	<b>ip igmp snooping vlan <i>vlan-id</i> querier query-interval <i>interval-value</i></b>	Optional By default, the query interval of the general group is 125 seconds

---

 **Note**

- In the same VLAN, the configured query interval of the general group should be larger than the maximum response time. Otherwise, the configuration cannot succeed.
- 

### Configure Max. Response Time

The general group query packet sent by IGMPv2 querier contains the maximum response time field. The multicast receiver sends the member report packets within the maximum response interval. If the multicast receiver does not send the member report packets within the maximum response time, the device regards that the subnet does not have the receiver of the multicast group and then deletes the multicast group information at once.

Table 65-8 Configuring Maximum Response Time

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure Max. Response Time	<b>ip igmp snooping vlan <i>vlan-id</i> querier max-response-time <i>time-value</i></b>	Optional By default, the maximum response time is 10 seconds

## Note

- In the same VLAN, the configured maximum response time should be smaller than the query interval of the general group. Otherwise, the configuration cannot succeed.

### Configure Query Interval of Specified Group

When the IGMP querier receives the leave packet of one multicast group, it sends the query packet of the specified group to query the segment for the multicast group, so as to know whether the subnet has the member of the multicast group. If not receiving the member report packet of the multicast group after waiting for “maximum response time”, delete the information of the multicast group.

Table 65-9 Configuring Query Interval of Specified Group

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure Query Interval of Specified Group	<b>ip igmp snooping vlan <i>vlan-id</i> last-member-query-interval <i>interval-value</i></b>	Optional By default, the query interval of the specified group is 1000 milliseconds

### Configure Fast Leave

If the device receives the leave packet of one multicast group after configuring fast leave, the device does not send the query packet of the specified group to the port any more and the information of the multicast group is deleted at once.

Table 65-10 Configuring Fast Leave

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure Fast Leave	<b>ip igmp snooping vlan <i>vlan-id</i> immediate-leave</b>	Mandatory By default, the fast leave function of the specified VLAN is disabled

---

## Note

- There are multiple receivers of the same multicast group in the device port at the same time. When the port receives the IGMP leave packet of the multicast group sent by one receiver and if fast leave is configured in the VLAN of the device port, the multicast services of the other receivers are interrupted.
- 

### 65.2.3 Configure IGMP snooping Router Port

IGMP snooping router port is the port receiving IGMP group query packets or multicast routing protocol packets. When the device receives the IGMP member report or leave packet, forward the packet via IGMP snooping router port. In this way, the upper-connected router can maintain the IGMP member relation table correctly.

IGMP snooping router port can be dynamically learned or configured manually. IGMP snooping dynamic router port refreshes the age time by regularly receiving the IGMP group query packets or multicast routing protocol packets. IGMP snooping static router port does not age.

#### Configuration Condition

Before configuring the IGMP snooping router port functions, first complete the following tasks:

- Enable global and VLAN IGMP snooping function
- Add port member in VLAN

#### Configure IGMP snooping Static Router Port

After configuring IGMP snooping static router port, the device can forward the IGMP protocol packet via the port even the port does not receive the IGMP group query packet or multicast routing protocol packet. It can prevent the problem that the router port ages because the services of the upper-connected L3 multicast device are interrupted.

Table 65-11 Configuring IGMP snooping Static Router Port

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure IGMP snooping Static Router Port	<b>ip igmp snooping vlan <i>vlan-id</i> mrouter interface { <i>interface-name</i>   link-aggregation <i>link-aggregation-id</i> }</b>	Mandatory  By default, the IGMP snooping static router port is not configured

### Configure age time for the IGMP snooping dynamic router port

As long as the configured age time for the IGMP snooping dynamic router port is longer, the problem can be effectively prevented that the router port ages fast because the services of the uplink L3 multicast device are interrupted.

Table 65-12 Configuring Age Time for IGMP Snooping Dynamic Router Port

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure age time for the IGMP snooping dynamic router port	<b>ip igmp snooping vlan <i>vlan-id</i> timer router-port expiry <i>expiry-value</i></b>	Optional  By default, the age time of the IGMP snooping dynamic router port is 255 seconds

## 65.2.4 Configure the IGMP snooping TCN event

### Configuration Condition

Before configuring the IGMP snooping TCN event function, do the following:

- Enable global and VLAN IGMP snooping function

### Enable fast convergence

When the network topology varies, a TCN event will be generated. The root port of the spanning tree will actively send a global IGMP leave packet (group address: 0.0.0.0) to request the IGMP querier in order to send a general group query packet, achieving fast convergence.

After you enable the fast convergence of the IGMP snooping TCN event, the root port of the non-spanning tree can also actively send a global IGMP leave packet (group address: 0.0.0.0), achieving the fast convergence.

Table 65-13 Enabling Fast Convergence

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable fast convergence	<b>ip igmp snooping tcn query solicit</b>	Mandatory  By default, fast convergence is disabled in the TCN event

### Configure TCN event query interval

When the TCN event occurs, the IGMP snooping querier will send a general group query at the TCN event query interval.

Table 65-14 Configuring TCN Event Query Interval

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure TCN event query interval	<b>ip igmp snooping vlan <i>vlan-id</i> querier tcn query interval <i>interval-value</i></b>	Optional  By default, the TCN event query interval is 31 seconds

### Configure TCN event query count

When the TCN event occurs, the IGMP snooping querier will send a general group query at the TCN event query interval, and will restore to the general group query interval after the number of sending times reaches the configured TCN event query count.

Table 65-15 Configuring Number of TCN Event Queries

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure TCN event query count	<b>ip igmp snooping vlan <i>vlan-id</i> querier tcn query count <i>count-number</i></b>	Optional By default, the TCN event query count is 2

### 65.2.5 Configure the IGMP snooping policy

The IGMP snooping policy is mainly used to control the receiver on the port, thereby controlling the multicast flow and restricting the receiver's behavior. The IGMP snooping policy can also be applied in the established L2 multicast flow forwarding environment.

#### Configuration Condition

Before configuring the IGMP snooping policy, do the following:

- Enable global and VLAN IGMP snooping function

#### Configure the port filtering rules

When expecting to obtain multicast services, the receiver may actively initiate an IGMP member report packet, and the device will make a judgment according to the port filtering rules applied under the port: deny the user to join the destination multicast group; allow the user to join the destination multicast group; and limit the number of times and duration that the user joins the destination multicast group.

Table 65-16 Configuring Port Filtering Rules

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the IGMP profile configuration mode	<b>ip igmp profile <i>profile-id</i></b>	-
Configure the range of denying multicast groups	<b>deny { all   <i>low-ip-address</i> [ <i>high-ip-address</i> ] }</b>	Optional By default, the range of denying multicast groups is not configured

Step	Command	Description
Configure the range of permitting multicast groups	<b>permit</b> { <b>all</b>   <i>low-ip-address</i> [ <i>high-ip-address</i> ] }	Optional By default, the range of permitting multicast groups is not configured
Configure preview rules for multicast groups	<b>preview</b> { <b>all</b>   <i>low-ip-address</i> [ <i>high-ip-address</i> ]   <b>count</b> <i>count-number</i>   <b>interval</b> <i>interval-time</i>   <b>time</b> <i>time-duration</i> }	Optional By default, the preview rules for multicast groups are not configured
Return to the global configuration mode	<b>exit</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2 Ethernet interface
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Apply the IGMP port filtering rules under the port	<b>ip igmp filter</b> <i>profile-number</i>	Mandatory By default, the IGMP port filtering rules are not applied under the port

## Note

- The multicast group address can only be in one of the IGMP profile filtering rules: deny, permit, and preview. The new rule overrides the old rule.
- Reset cycle of preview count > preview duration × preview count + preview interval × (preview count - 1).

### Configure the maximum number of port multicast group entries

The maximum number of port multicast group entries can limit the number of receivers joining the multicast groups.

Table 65-17 Maximum Number of Port Multicast Group Entries

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2 Ethernet interface
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Configure the maximum number of the port multicast group entries under the port	<b>ip igmp max-groups</b> <i>number</i>	Optional  By default, the maximum number of the multicast group entries that can dynamically join the port is 6144

### Configure the upper limit policy of port multicast groups

In the case that the number of the multicast groups the receiver joins exceeds the configured maximum number of multicast group entries, if the upper limit policy of port multicast groups is replace, the newly joined multicast group on the device automatically replaces the existing multicast group, and if the upper limit policy of port multicast groups is deny, the newly joined multicast group is denied.

Table 65-18 Configuring Upper Limit Policy of Port Multicast Groups

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Configure the upper limit policy of port multicast groups	<b>ip igmp max-groups action</b> { <b>deny</b>   <b>replace</b> }	Optional  By default, when the number of the multicast group entries that dynamically join the port reaches the maximum, the handling action is reject new entries

### Configure Interface Control for PIM JOIN Packet

After Configure Interface for Control PIM JOIN Packet is enabled, the JOIN packet runs through not hardware but software.

Table 65-19 Configuring Interface Control for PIM JOIN Packet

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure Interface Control for PIM JOIN Packet	<b>ip igmp snooping vlan</b> <i>vlan-id</i> <b>ctrl-pim</b>	Mandatory

Step	Command	Description
		By default, the PIM JOIN packet of the specified VLAN is not controlled

## Note

- The VLAN will be flooded with the JOIN packets before enabling, and after enabling, the CPU will be captured and the VLAN will not be flooded.

### 65.2.6 Configure IGMP snooping Proxy

When there are many multicast group receivers in the network, you can configure IGMP snooping Proxy on the device in order to reduce the quantity of IGMP member reports and leave packets received by the upstream multicast device and effectively reduce the system overhead.

IGMP snooping Proxy can act as proxy of downstream receivers to send IGMP member report packets and leave packets to upstream devices; it can also respond to the IGMP group query packets sent by the upstream multicast devices, and then send the IGMP group query packets to the downstream devices.

#### Configuration Condition

Before configuring the IGMP snooping function, do the following:

- Enable global and VLAN IGMP snooping function

#### Configure IGMP snooping Proxy

Table 65-20 Configuring IGMP snooping Proxy

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure IGMP snooping Proxy	<b>ip igmp snooping proxy</b> <b>vlan <i>vlan-id</i> upstream</b> <b>interface { <i>interface-name</i>  </b> <b>link-aggregation <i>link-</i></b> <b>aggregation-id }</b>	Mandatory By default, no IGMP proxy port in the VLAN is configured

## 65.2.7 Configure IGMP snooping Static Group

IGMP snooping static groups are static IGMP snooping group entries generated by means of static configuration. By configuring the IGMP snooping static groups, the aging problem of the multicast groups dynamically learned by IGMP snooping can be effectively solved.

When the device is configured with the IGMP snooping static group in the VLAN, the IGMP snooping querier and querier address in the VLAN, and the IGMP snooping proxy port in the VLAN, the device will generate static IGMP snooping groups entries and send the IGMP member report packet to the IGMP snooping proxy port in the VLAN. The source IP address of this IGMP member report packet is the configured querier address. In this way, the uplink router can correctly maintain the IGMP membership table. When you delete the IGMP snooping static group configuration in the VLAN, the device will delete the corresponding IGMP snooping static group entries and send an IGMP member leave packet to the IGMP snooping proxy port in the VLAN.

### Configuration Condition

Before configuring the IGMP snooping static group function, do the following:

- Enable global and VLAN IGMP snooping function
- Add port member in VLAN

### Configure IGMP snooping Static Group

Table 65-21 Configuring IGMP snooping Static Group

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure IGMP snooping Static Group	<b>ip igmp snooping vlan <i>vlan-id</i> static-group <i>group-ip-address</i> { interface <i>interface-name</i>   interface <b>link-aggregation</b> <i>link-aggregation-id</i> }</b>	Mandatory By default, the IGMP snooping static group in the VLAN is not configured

## 65.2.8 Monitoring and Maintaining of IGMP Snooping

Table 65-6565 Monitoring and Maintaining of IGMP Snooping

Command	Description
<b>clear ip igmp snooping groups</b> [ grp-addr ip-address   vlan vlan-id [ grp-addr ip-address-in-vlan ] ]	Clear IGMP snooping group information
<b>clear ip igmp snooping statistics</b> vlan vlan-id [ interface interface-name   interface link-aggregation link-aggregation-id ]	Clear statistics of IGMP protocol packets
<b>show ip igmp snooping proxy member database</b> [ vlan vlan-id ]	Show IGMP snooping proxy member database information
<b>show ip igmp snooping proxy special query source-list</b> [ vlan vlan-id ]	Show the source list of the specified source queries received by IGMP snooping proxy
<b>show ip igmp snooping proxy upstream</b> [ vlan vlan-id ]	Show the running information of IGMP snooping proxy
<b>show ip igmp snooping debugging</b>	Show IGMP snooping debugging status information
<b>show ip igmp snooping egress_table</b>	Show the IGMP snooping L2 forwarding table
<b>show ip igmp snooping groups</b> [ vlan vlan-id ] [ grp-addr ip-address ]	Show IGMP snooping multicast groups information
<b>show ip igmp snooping groups</b> [ vlan vlan-id ] count	Show the count of the IGMP snooping multicast groups information
<b>show ip igmp snooping groups detail</b> [ vlan vlan-id ] [ grp-addr ip-address ]	Show the detail of IGMP snooping multicast groups
<b>show ip igmp snooping interface statistics</b>	Show statistics about the count of multicast groups joining the IGMP snooping port
<b>show ip igmp snooping l3_ip_table</b>	Show the IGMP snooping L3 forwarding table
<b>show ip igmp snooping mcast_table</b>	Show the IGMP snooping forwarding table
<b>show ip igmp snooping mrouter</b> [ vlan vlan-id ]	Show IGMP snooping router port information

Command	Description
<b>show ip igmp snooping querier</b> [ <i>vlan vlan-id</i> ]	Show IGMP snooping querier information
<b>show ip igmp snooping statistics</b> <i>vlan vlan-id</i> [ <b>interface</b> <i>interface-name</i>   <b>interface link-aggregation</b> <i>link-aggregation-id</i> ]	Show statistics about IGMP packets of the IGMP snooping port
<b>show ip igmp snooping</b> [ <i>vlan vlan-id</i> [ <b>info</b> ] ]	Show IGMP snooping information
<b>show multicast control</b> [ <b>all-info</b>   <b>interface</b> <i>interface-name</i>   <b>interface link-aggregation</b> <i>link-aggregation-id</i> ]	Show L2 multicast control information

## 65.3 Typical Configuration Examples of IGMP Snooping

### 65.3.1 Configure IGMP Snooping

#### Network Requirements

- On Device 1, configure the multicast routing protocol, on Device 2, enable IGMP snooping, PC 1 and PC 2 are the receivers of multicast services, and PC 3 is a receiver of non-multicast services.
- Multicast Server sends the multicast service packets, PC 1 and PC 2 can correctly receive the multicast service packets, and PC 3 cannot receive the multicast service packets.

#### Network Topology

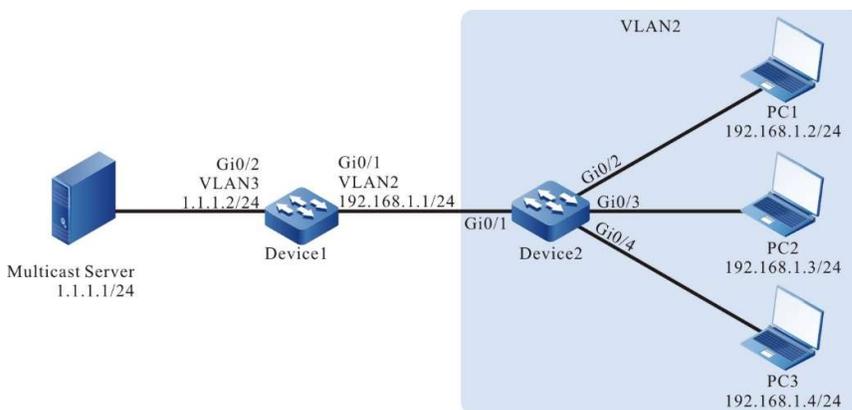


Figure 65-1 Network Topology for configuring IGMP Snooping

## Configuration Steps

Step 1: On Device 1, configure the interface IP address and enable the multicast routing protocol.  
(Omitted)

Step 2: Configure Device2.

Create VLAN2 on #Device 2.

```
Device2#configure terminal
Device2(config)#vlan 2
Device2(config-vlan2)#exit
```

#On Device 2, configure the link type of ports gigabitethernet0/2-gigabitethernet0/4 to Access to allow services of VLAN 2 to pass.

```
Device2(config)#interface gigabitethernet 0/2-0/4
Device2(config-if-range)#switchport access vlan 2
Device2(config-if-range)#exit
```

#On Device 2, configure the link type of port gigabitethernet0/1 to Trunk to allow services of VLAN 2 to pass, and configure PVID to 1.

```
Device2(config)#interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#switchport mode trunk
Device2(config-if-gigabitethernet0/1)#switchport trunk allowed vlan add 2
Device2(config-if-gigabitethernet0/1)#switchport trunk pvid vlan 1
Device2(config-if-gigabitethernet0/1)#exit
```

#Enable unknown multicast drop in VLAN 2.

```
Device2(config)#vlan 2
Device2(config-vlan2)#l2-multicast drop-unknown
Device2(config-vlan2)#l3-multicast drop-unknown
Device2(config-vlan2)#exit
```

#Enable IGMP Snooping.

```
Device2(config)#ip igmp snooping
Device2(config)#ip igmp snooping vlan 2
```

Step 3: Check the result.

#PC 1 and PC 2 send IGMPv2 member report packets to join the multicast group 224.1.1.1.

#View the multicast membership table of Device 2.

```
Device2#show ip igmp snooping groups
VLAN ID Interface Name Group Address Expires Last Reporter V1 Expires V2 Expires Uptime
```

```

2    gi0/2    224.1.1.1  00:03:26  192.168.1.2  stopped    00:00:55
2    gi0/3    224.1.1.1  00:03:44  192.168.1.3  stopped    00:00:40

```

#Multicast Server sends the multicast service packet with the destination address of 224.1.1.1, PC 1 and PC 2 can correctly receive the multicast service packet, and PC 3 cannot receive the multicast service packet.

### 65.3.2 Configure Multicast Receiving Control

#### Network Requirements

- On Device 1, configure the multicast routing protocol.
- Device 2 enables IGMP snooping, configures multicast receiving control and applies it to the corresponding port.
- Multicast Server sends the multicast service packets, and PC 1 and PC 2 can correctly receive the multicast service packets.

#### Network Topology

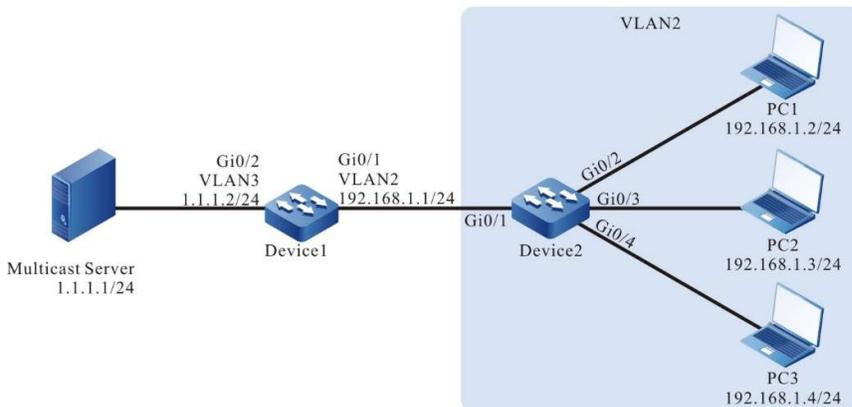


Figure 65-2 Network Topology for configuring Multicast Receiving Control

#### Configuration Steps

Step 1: On Device 1, configure the interface IP address and enable the multicast routing protocol.  
(Omitted)

Step 2: Configure Device2.

#Create VLAN2 on Device2.

```

Device2#configure terminal
Device2(config)#vlan 2
Device2(config-vlan2)#exit

```

#On Device 2, configure the link type of ports gigabitethernet0/2-gigabitethernet0/4 to Access to allow services of VLAN 2 to pass.

```
Device2#configure terminal
Device2(config)#vlan 2
Device2(config-vlan2)#exit
Device2(config)#interface gigabitethernet 0/2-0/4
Device2(config-if-range)#switchport access vlan 2
Device2(config-if-range)#exit
```

#On Device 2, configure the link type of port gigabitethernet0/1 to Trunk to allow services of VLAN 2 to pass, and configure PVID to 1.

```
Device2(config)#interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#switchport mode trunk
Device2(config-if-gigabitethernet0/1)#switchport trunk allowed vlan add 2
Device2(config-if-gigabitethernet0/1)#switchport trunk pvid vlan 1
Device2(config-if-gigabitethernet0/1)#exit
```

#Enable IGMP Snooping.

```
Device2(config)#ip igmp snooping
Device2(config)#ip igmp snooping vlan 2
```

#Configure multicast receiving control policy profile1 to allow joining the multicast group 224.1.1.1 and apply it to port gigabitethernet0/2.

```
Device2(config)#ip igmp profile 1
Device2(config-igmp-profile)#permit 224.1.1.1
Device2(config-igmp-profile)#exit
Device2(config)#interface gigabitethernet 0/2
Device2(config-if-gigabitethernet0/2)#ip igmp filter 1
Device2(config-if-gigabitethernet0/2)#exit
```

#Configure multicast receiving control policy profile2 to allow previewing the multicast group 224.1.1.1 and apply it to port gigabitethernet0/3.

```
Device2(config)#ip igmp profile 2
Device2(config-igmp-profile)#preview 224.1.1.1
Device2(config-igmp-profile)#exit
Device2(config)#interface gigabitethernet 0/3
Device2(config-if-gigabitethernet0/3)#ip igmp filter 2
Device2(config-if-gigabitethernet0/3)#exit
```

#Configure multicast receiving control policy profile3 to deny joining the multicast group 224.1.1.1 and apply it to port gigabitethernet0/4.

```
Device2(config)#ip igmp profile 3
Device2(config-igmp-profile)#permit all
```

```

Device2(config-igmp-profile)#deny 224.1.1.1
Device2(config-igmp-profile)#exit
Device2(config)#interface gigabitethernet 0/4
Device2(config-if-gigabitethernet0/4)#ip igmp filter 3
Device2(config-if-gigabitethernet0/4)#exit

```

Step 3: Check the result.

#PC 1, PC 2, and PC 3 send IGMPv2 member report packets to join the multicast group 224.1.1.1.

#View the multicast membership table of Device 2.

```

Device2#show ip igmp snooping groups
IGMP Snooping Group Membership
Total 2 groups

VLAN ID Interface Name Group Address Expires Last Reporter V1 Expires V2 Expires Uptime
-----
2    gi0/2    224.1.1.1  00:04:19 192.168.1.2 stopped    00:00:01
2    gi0/3    224.1.1.1  00:04:19 192.168.1.3 stopped    00:00:01

```

PC 1 and PC 2 can join the multicast group 224.1.1.1, and PC3 does not join the multicast group 224.1.1.1.

#Multicast Server sends the multicast service packet with the destination address of 224.1.1.1.

PC 1 and PC 2 can correctly receive the multicast service packet, and PC 3 cannot receive the multicast service packet.

#After 10 seconds, view the multicast membership table of Device 2 and gigabitethernet0/3 multicast receiving control information.

```

Device2#show ip igmp snooping groups
IGMP Snooping Group Membership
Total 1 group

VLAN ID Interface Name Group Address Expires Last Reporter V1 Expires V2 Expires Uptime
-----
2    gi0/2    224.1.1.1  00:04:10 192.168.1.2 stopped    00:00:10

Device2#show multicast control interface gigabitethernet 0/3
ip multicast control gigabitethernet0/3 vlan 2 information
-----
profile: 2
group right information:
  preview: 224.1.1.1
preview information:

```

preview count: 3  
preview count remain: 2  
preview time: 10 (s)  
preview interval: 60 (s)  
group information:  
group: 224.1.1.1  
uptime: 00:00:10  
next preview time remain: 00:00:60

When the preview time of gigabitethernet0/3 port expires (10 s later), the group membership table entry is deleted, PC1 can correctly receive multicast service packets, and PC 2 and PC 3 cannot receive multicast service packets.

### 65.3.3 Configure IGMP snooping Proxy

#### Network Requirements

- On Device 1, configure the multicast routing protocol.
- Enable IGMP snooping and IGMP Snooping Proxy on Device 2.
- Multicast Server sends the multicast service packets, and PC 1, PC 2 and PC 3 can correctly receive the multicast service packets.

#### Network Topology

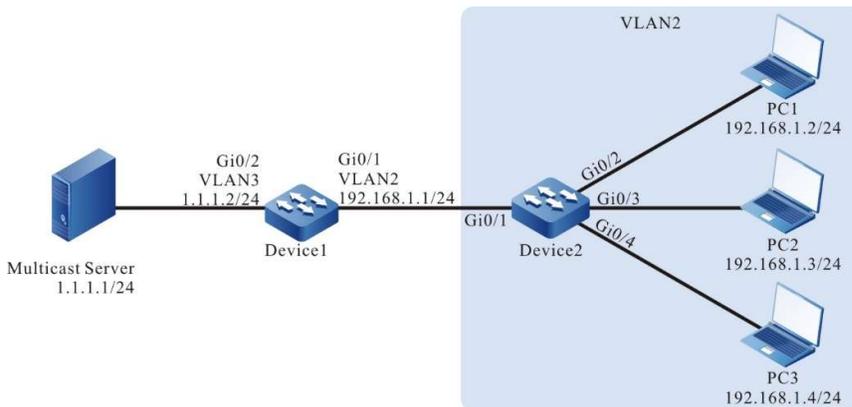


Figure 65-3 Network Topology for configuring IGMP Snooping Proxy

#### Configuration Steps

Step 1: On Device 1, configure the interface IP address and enable the multicast routing protocol.

```
Device1#configure terminal
Device1(config)#ip multicast-routing
Device1(config)#interface gigabitethernet0/1
```

```

Device1(config-if-gigabitethernet0/1)# switchport mode trunk
Device1(config-if-gigabitethernet0/1)# witchport trunk allowed vlan add 2
Device1(config-if-gigabitethernet0/1)# switchport trunk pvid vlan 1
Device1(config-if-gigabitethernet0/1)# exit
Device1(config)#interface gigabitethernet0/2
Device1(config-if-gigabitethernet0/2)# switchport mode trunk
Device1(config-if-gigabitethernet0/2)# witchport trunk allowed vlan add 3
Device1(config-if-gigabitethernet0/2)# switchport trunk pvid vlan 1
Device1(config-if-gigabitethernet0/2)# exit
Device1(config)#interface vlan 2
Device1(config-if-vlan2)# ip address 192.168.1.1 255.255.255.0
Device1(config-if-vlan2)# ip pim sparse-mode
Device1(config-if-vlan2)# exit
Device1(config)#interface vlan 3
Device1(config-if-vlan3)# ip address 1.1.1.2 255.255.255.0
Device1(config-if-vlan3)# ip pim sparse-mode
Device1(config-if-vlan3)# exit

```

## Step 2: Configure Device2.

### #Create VLAN2 on Device2.

```

Device2#configure terminal
Device2(config)#vlan 2
Device2(config-vlan2)#exit

```

#On Device 2, configure the link type of ports gigabitethernet0/2-gigabitethernet0/4 to Access to allow services of VLAN 2 to pass.

```

Device2(config)#interface gigabitethernet 0/2-0/4
Device2(config-if-range)#switchport access vlan 2
Device2(config-if-range)#exit

```

#On Device 2, configure the link type of port gigabitethernet0/1 to Trunk to allow services of VLAN 2 to pass, and configure PVID to 1.

```

Device2(config)#interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#switchport mode trunk
Device2(config-if-gigabitethernet0/1)#switchport trunk allowed vlan add 2
Device2(config-if-gigabitethernet0/1)#switchport trunk pvid vlan 1
Device2(config-if-gigabitethernet0/1)#exit

```

#Enable in VLAN2, IGMP snooping and configure the IGMP snooping querier address as 192.168.1.254.

```

Device2(config)#ip igmp snooping

```

```

Device2(config)#ip igmp snooping vlan 2
Device2(config)#ip igmp snooping vlan 2 querier
Device2(config)#ip igmp snooping vlan 2 querier address 192.168.1.254

```

### #Configure IGMP snooping Proxy.

```

Device2(config)#ip igmp snooping proxy vlan 2 upstream interface gigabitethernet 0/1
Device2(config)#exit

```

Step 3: Check the result.

#PC 1, PC 2 and PC 3 in turn send IGMPv2 member report packets to join the multicast group 224.1.1.1.

#View the IGMP Snooping Proxy information of Device 2.

```

Device2#show ip igmp snooping proxy upstream vlan 2
vlan 2 proxy upstream information:
-----
upstream interface          : gi0/1
upstream querier compatmode version : 2
upstream querier address    : 192.168.1.1
upstream report source address : 192.168.1.254
upstream querier query interval : 125s
upstream querier query response interval: 10s
upstream querier LMQUI      : 1s
upstream querier LMQC      : 2
upstream querier robustness variable : 2
upstream querier present timer : 00:02:50
upstream V1 querier present timer : stopped
upstream V2 querier present timer : 00:02:55

```

#View the Device 2 multicast membership table and the IGMP Snooping Proxy member database.

```

Device2#show ip igmp snooping groups
IGMP Snooping Group Membership
Total 3 groups

VLAN ID Interface Name Group Address Expires Last Reporter V1 Expires V2 Expires Uptime
-----
2   gi0/2   224.1.1.1  00:04:09 192.168.1.2 stopped 00:00:14
2   gi0/3   224.1.1.1  00:04:09 192.168.1.3 stopped 00:00:11
2   gi0/4   224.1.1.1  00:04:12 192.168.1.4 stopped 00:00:07

```

It is indicated that PC 1, PC 2, and PC 3 join the multicast group 224.1.1.1.

```

Device2#show ip igmp snooping proxy member database vlan 2

```

IGMP Snooping Proxy Member Database Table

Total 1 group

VLAN ID	Group Address	Mode	Source Address
---------	---------------	------	----------------

2	224.1.1.1	EXCLUDE *	
---	-----------	-----------	--

#View the multicast membership table of Device 1.

Device1#show ip igmp groups

IGMP Connected Group Membership

Total 1 groups

Group Address	Interface	Uptime	Expires	Last Reporter	V1 Expires	V2 Expires
---------------	-----------	--------	---------	---------------	------------	------------

224.1.1.1	vlan 2	00:00:15	00:04:11	192.168.1.254	stopped	
-----------	--------	----------	----------	---------------	---------	--

It is indicated that when PC joins the multicast group 224.1.1.1, Device 2 only forwards the first IGMPv2 member report packet to Device 1, and drops all other packets.

#Multicast Server sends the multicast service packet with the destination address of 224.1.1.1, PC 1, PC 2 and PC 3 can correctly receive the multicast service packet.

PC 1 and PC 2 send an IGMPv2 leave packet to leave the multicast group 224.1.1.1.

Device2#show ip igmp snooping groups

IGMP Snooping Group Membership

Total 1 group

VLAN ID	Interface Name	Group Address	Expires	Last Reporter	V1 Expires	V2 Expires	Uptime
---------	----------------	---------------	---------	---------------	------------	------------	--------

2	gi0/4	224.1.1.1	00:03:54	192.168.1.4	stopped		00:06:37
---	-------	-----------	----------	-------------	---------	--	----------

Device1#show ip igmp groups

IGMP Connected Group Membership

Total 1 groups

Group Address	Interface	Uptime	Expires	Last Reporter	V1 Expires	V2 Expires
---------------	-----------	--------	---------	---------------	------------	------------

224.1.1.1	vlan 2	00:06:48	00:03:48	192.168.1.2	stopped	
-----------	--------	----------	----------	-------------	---------	--

After PC 1 and PC 2 leave the multicast group 224.1.1.1, because PC 3 has not left this multicast group with the group member PC 3 still being in the multicast membership table, Device 2 will not send a leave packet of this multicast group to Device 1.

#PC 3 sends an IGMPv2 leave packet to leave the multicast group 224.1.1.1, and views the multicast membership tables of Device 2 and Device 1.

Device2#show ip igmp snooping groups

It is indicated that there is no multicast membership table on Device 2.

Device1#show ip igmp groups

There are no multicast members on Device 1. When PC 3, the last group member, leaves the multicast group, Device 2 will send a leave packet of this multicast group to Device 1.

#PC 1, PC 2 and PC 3 cannot receive the multicast service packet.

### 65.3.4 Configure Unknown Multicast Redirection

#### Network Requirements

- On Device 2, configure the multicast routing protocol.
- Enable IGMP snooping, unknown multicast drop and unknown multicast redirection on Device 1.
- Multicast Server sends the multicast service packets, and PC 1, PC 2 and PC 3 can correctly receive the multicast service packets.

#### Network Topology

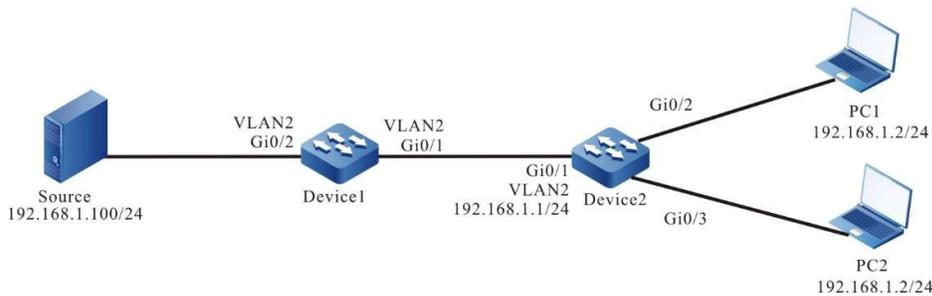


Figure 65-4 Network Topology for configuring Unknown Multicast Redirect

#### Configuration Steps

Step 1: On Device 2, configure the interface IP address and enable the multicast routing protocol.  
(Omitted)

Step 2: Configure Device 2 and Device 1.

#On Device 2, configure the link type of ports gigabitethernet0/2-gigabitethernet0/3 to Access to allow services of VLAN 2 to pass, and configure the link type of port gigabitethernet0/1 to Trunk to allow services of VLAN 2 to pass. Configure PVID to 1.

```
Device2(config)#interface gigabitethernet 0/2-0/3
Device2(config-if-range)#switchport access vlan 2
Device2(config-if-range)#exit
Device2(config)#interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#switchport mode trunk
Device2(config-if-gigabitethernet0/1)#switchport trunk allowed vlan add 2
Device2(config-if-gigabitethernet0/1)#switchport trunk pvid vlan 1
```

```
Device2(config-if-gigabitethernet0/1)#exit
Device2(config-if-vlan2)# ip address 192.168.1.1 255.255.255.0
Device1(config-if-vlan2)# ip pim sparse-mode
Device1(config-if-vlan2)# exit
```

#### #Create VLAN 2 on Device 1.

```
Device2#configure terminal
Device2(config)#vlan 2
Device2(config-vlan2)#exit
```

#On Device 1, configure the link type of port gigabitethernet0/2 to Access to allow services of VLAN 2 to pass, and configure the link type of port gigabitethernet0/1 to Trunk to allow services of VLAN 2 to pass. Configure PVID to 1.

```
Device1(config)#interface gigabitethernet 0/2
Device1(config-if-gigabitethernet0/2)# switchport access vlan 2
Device1(config-if-gigabitethernet0/2)#exit
Device1(config)#interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#switchport mode trunk
Device1(config-if-gigabitethernet0/1)#switchport trunk allowed vlan add 2
Device1(config-if-gigabitethernet0/1)#switchport trunk pvid vlan 1
Device1(config-if-gigabitethernet0/1)#exit
```

#### #Enable unknown multicast drop in VLAN 2.

```
Device1(config)#vlan 2
Device1(config-vlan2)#l2-multicast drop-unknown
Device1(config-vlan2)#l3-multicast drop-unknown
Device1(config-vlan2)#exit
```

#### #Enable IGMP Snooping.

```
Device1(config)#ip igmp snooping
Device1(config)#ip igmp snooping vlan 2
```

#### #Enable unknown multicast redirection in VLAN 2.

```
Device1(config)#vlan 2
Device1(config-vlan2)#multicast mrouter-forwarding
Device1(config-vlan2)#exit
```

Step 3: Check the result.

#PC 1 and PC 2 send IGMPv2 member report packets to join the multicast group 224.1.1.1.

#View the multicast membership table of Device 2.

```
Device1#show ip igmp groups
```

IGMP Connected Group Membership

Total 1 groups

Group Address	Interface	Uptime	Expires	Last Reporter	V1 Expires	V2 Expires
224.1.1.1	vlan2	00:21:02	00:03:47	192.168.1.2	stopped	

#Multicast Server sends the multicast service packet with the destination address of 224.1.1.1, PC 1 and PC 2 can correctly receive the multicast service packet.

### 65.3.5 Configure IGMP snooping Static Group

#### Network Requirements

- On Device 1, configure the multicast routing protocol, on Device 2, enable IGMP snooping in VLAN 2, PC 1 and PC 2 are the receivers of IGMP snooping static group services, and PC 3 is not a receiver of multicast services.
- Multicast Server sends the multicast service packets, PC 1 and PC 2 can correctly receive the multicast service packets, and PC 3 cannot receive the multicast service packets.

#### Network Topology

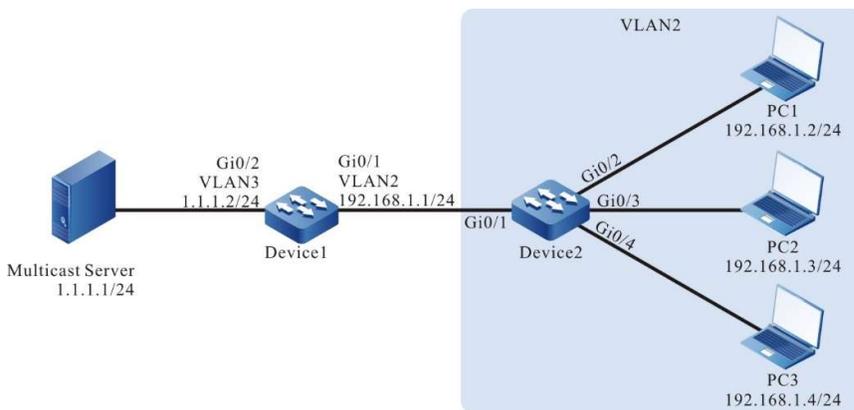


Figure 65-5 Network Topology for configuring IGMP Snooping Static Group

#### Configuration Steps

Step 1: On Device 1, configure the interface IP address and enable the multicast routing protocol. (Omitted)

Step 2: Configure Device2.

Create VLAN2 on #Device 2.

```
Device2#configure terminal
```

```
Device2(config)#vlan 2
```

```
Device2(config-vlan2)#exit
```

#On Device 2, configure the link type of ports gigabitethernet0/2-gigabitethernet0/4 to Access to allow services of VLAN 2 to pass.

```
Device2(config)#interface gigabitethernet 0/2-0/4
Device2(config-if-range)#switchport access vlan 2
Device2(config-if-range)#exit
```

#On Device 2, configure the link type of port gigabitethernet0/1 to Trunk to allow services of VLAN 2 to pass, and configure PVID to 1.

```
Device2(config)#interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#switchport mode trunk
Device2(config-if-gigabitethernet0/1)#switchport trunk allowed vlan add 2
Device2(config-if-gigabitethernet0/1)#switchport trunk pvid vlan 1
Device2(config-if-gigabitethernet0/1)#exit
```

#Enable unknown multicast drop in VLAN 2.

```
Device2(config)#vlan 2
Device2(config-vlan2)#12-multicast drop-unknown
Device2(config-vlan2)#13-multicast drop-unknown
Device2(config-vlan2)#exit
```

#Enable IGMP snooping and configure IGMP snooping static group.

```
Device2(config)#ip igmp snooping
Device2(config)#ip igmp snooping vlan 2
Device2(config)#ip igmp snooping vlan 2 static-group 224.1.1.1 interface gigabitethernet 0/2
Device2(config)#ip igmp snooping vlan 2 static-group 224.1.1.1 interface gigabitethernet 0/3
Device2(config)#exit
```

Step 3: Check the result.

#View the multicast membership table of Device 2.

```
Device2#show ip igmp snooping groups
IGMP Snooping Static Group Membership
Total 2 group

VLAN ID  Port Name      Group Address  Uptime
-----  -
2        gi0/2          224.1.1.1     00:00:48
2        gi0/3          224.1.1.1     00:00:45
```

#Multicast Server sends the multicast service packet with the destination address of 224.1.1.1, PC 1 and PC 2 can correctly receive the multicast service packet, and PC 3 cannot receive the multicast service packet.

# 66 Multicast VLAN

---

## 66.1 Overview

In the traditional L2 multicast on-demand mode, when users in different VLANs request on-demand, each VLAN will replicate a multicast stream in the same VLAN. This multicast on-demand mode wastes a lot of bandwidth.

To solve this problem, you can configure a multicast VLAN so that users in different VLANs share one multicast VLAN. After the multicast VLAN function is enabled, the multicast stream is transmitted only in the multicast VLAN, and the multicast VLAN is completely isolated from the user VLAN. This not only saves bandwidth but also ensures security.

There are two types of multicast VLAN: MVR (Multicast VLAN Registration) and MVP (Multicast VLAN Plus).

## 66.2 Multicast VLAN Configuration

Table 66-1 Multicast VLAN Configuration

Configuration Task	
Configure MVP	Configure MVP Multicast VLAN
	Enable MVP function
Configure MVR	Configure MVR multicast VLAN
	Enable MVR function

### 66.2.1 Configure MVP

MVP is used in edge networks, and the sub-VLAN member ports can be connected to multicast devices or directly to users. When connected to a multicast device, a sub-VLAN member port can send multicast

packets with a VLAN tag; when connected to a user, the sub-VLAN member port can send multicast packets without VLAN tag.

### Configuration Condition

Before configuring MVP multicast VLAN, do the following:

- Configure the VLAN;
- Enable global and VLAN IGMP snooping function

### Configure MVP Multicast VLAN

You can configure MVP to implement cross-VLAN forwarding of multicast packets between the MVP multicast VLAN and member sub-VLANs. The member port of the MVP multicast VLAN needs to be consistent with the VLAN tag of the upstream device connected to it, and the member ports of the MVP sub-VLANs must be consistent with that the VLAN tag of the downstream device connected to it.

Table 66-2 Configuring MVP Multicast VLAN

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure MVP Multicast VLAN	<b>multicast-vlan</b> <i>mvlan-id</i> <b>subvlan</b> <i>subvlan-id</i>	Mandatory By default, no MVP multicast VLAN or member sub-VLANs are configured

### Enable MVP function

Only after the MVP function is enabled in the MVP multicast VLAN, can packets be forwarded across VLANs between the MVP multicast VLAN and the member sub-VLANs.

Table 66-3 Enabling MVP Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the VLAN configuration mode	<b>vlan</b> <i>vlan-id</i>	-

Step	Command	Description
Enable the MVP function in the VLAN	<b>multicast-vlan enable</b>	Mandatory By default, the MVP function is disabled in the VLAN

## 66.2.2 Configure MVR

MVR is used in edge networks. MVR multicast VLAN member port can only connect to users, and multicast packets sent from the VLAN member port cannot bear the VLAN tag.

### Configuration Condition

Before configuring MVR multicast VLAN, do the following:

- Configure the corresponding VLAN;
- Enable global and corresponding intra-VLAN IGMP snooping functions.

### Configure MVR multicast VLAN

When multiple user ports belong to different VLANs, these ports can be added to the MVR multicast VLAN, so that users in different VLANs can share one multicast VLAN.

Table 66-4 Configuring MVR Multicast VLAN

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure MVR multicast VLAN	<b>mvr vlan <i>vlan-id</i></b>	Mandatory By default, the MVP multicast VLAN is not configured

### Enable MVR function

Only after the MVR function is enabled, can the MVR multicast VLAN configuration take effect.

Table 66-5 Enabling MVR Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable MVR function	<b>mvr enable</b>	Mandatory By default, the MVR function is not enabled

### 66.2.3 Monitoring and Maintaining of Multicast VLAN

Table 66-6 Monitoring and Maintaining of Multicast VLAN

Command	Description
<b>show multicast-vlan</b> <i>vlan-id</i>	Show information of MVP multicast VLAN
<b>show mvr</b>	Show MVR information

## 66.3 Typical Configuration Examples of Multicast VLAN

### 66.3.1 Configure MVP

#### Network Requirements

- On Device 1, configure the multicast routing protocol.
- Device 2 enables IGMP snooping and configures MVP.
- Multicast Server sends multicast service packets, and multicast VLAN 2 can copy the multicast service packets to sub-VLAN 4 to sub-VLAN 5. PC 1, PC 2 and PC 3 can correctly receive the multicast service packets.

#### Network Topology

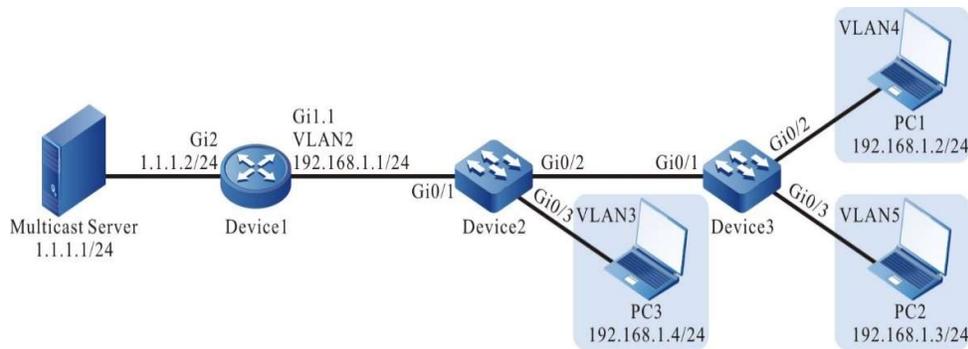


Figure 66-1 MVP Typical Configuration Network Topology

### Configuration Steps

Step 1: On Device 1, configure the interface IP address and enable the multicast routing protocol.  
(Omitted)

Step 2: Configure Device2.

#Create VLAN 2 to VLAN 5 on Device 2.

```
Device2#configure terminal
Device2(config)#vlan 2-5
```

#On Device 2, configure the link type of port gigabitethernet0/1 to Trunk to allow services of VLAN2 to pass, and configure PVID to 1.

```
Device2(config)#interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#switchport mode trunk
Device2(config-if-gigabitethernet0/1)#switchport trunk allowed vlan add 2
Device2(config-if-gigabitethernet0/1)# switchport trunk pvid vlan 1
Device2(config-if-gigabitethernet0/1)#exit
```

#On Device 2, configure the link type of port gigabitethernet0/2 to Trunk to allow services of VLAN 4 to VLAN 5 to pass, and configure PVID to 1.

```
Device2(config)#interface gigabitethernet 0/2
Device2(config-if-gigabitethernet0/2)#switchport mode trunk
Device2(config-if-gigabitethernet0/2)#switchport trunk allowed vlan add 4-5
Device2(config-if-gigabitethernet0/2)# switchport trunk pvid vlan 1
Device2(config-if-gigabitethernet0/2)#exit
```

#On Device 2, configure the link type of port gigabitethernet0/3 to Access to allow services of VLAN 3 to pass.

```
Device2(config)#interface gigabitethernet 0/3
Device2(config-if-gigabitethernet0/3)#switchport access vlan 3
Device2(config-if-gigabitethernet0/3)#exit
```

#Configure IGMP Snooping.

```
Device2(config)#ip igmp snooping
Device2(config)#ip igmp snooping vlan 2
Device2(config)#ip igmp snooping vlan 3
Device2(config)#ip igmp snooping vlan 4
Device2(config)#ip igmp snooping vlan 5
```

#### #Configure MVP.

```
Device2(config)#multicast-vlan 2 subvlan 3-5
Device2(config)#vlan 2
Device2(config-vlan2)#multicast-vlan enable
Device2(config-vlan2)#exit
```

#### Step 3: Configure Device 3.

#### #Create VLAN 4 to VLAN 5 on Device 3.

```
Device3#configure terminal
Device3(config)#vlan 4-5
```

#### #On Device 3, configure the link type of port gigabitethernet0/1 to Trunk to allow services of VLAN 4 to VLAN 5 to pass, and configure PVID to 1.

```
Device3(config)#interface gigabitethernet 0/1
Device3(config-if-gigabitethernet0/1)#switchport mode trunk
Device3(config-if-gigabitethernet0/1)#switchport trunk allowed vlan add 4-5
Device3(config-if-gigabitethernet0/1)# switchport trunk pvid vlan 1
Device3(config-if-gigabitethernet0/1)#exit
```

#### #On Device 3, configure the link type of port gigabitethernet0/2 to Access to allow services of VLAN 4 to pass.

```
Device3(config)#interface gigabitethernet 0/2
Device3(config-if-gigabitethernet0/2)#switchport access vlan 4
Device3(config-if-gigabitethernet0/2)#exit
```

#### #On Device 3, configure the link type of port gigabitethernet0/3 to Access to allow services of VLAN 5 to pass.

```
Device3(config)#interface gigabitethernet 0/3
Device3(config-if-gigabitethernet0/3)#switchport access vlan 5
Device3(config-if-gigabitethernet0/3)#exit
```

#### Step 4: Check the result.

#### #View MVP information.

```
Device2#show multicast-vlan
```

#### Multicast Vlan Table

```
-----  
VLAN ID: 2  
status: enable  
subvlan count: 3  
subvlan: 3-5
```

#PC 1, PC 2 and PC 3 send IGMPv2 membership reports to join the multicast group 224.1.1.1.

#View the multicast membership table of Device 2.

```
Device2#show ip igmp snooping groups
```

```
IGMP Snooping Group Membership
```

```
Total 3 groups
```

```
VLAN ID Interface Name Group Address Expires Last Reporter V1 Expires V2 Expires Uptime
```

VLAN ID	Interface Name	Group Address	Expires	Last Reporter	V1 Expires	V2 Expires	Uptime
3	gi0/3	224.1.1.1	00:03:54	192.168.1.4	stopped	00:01:18	
4	gi0/2	224.1.1.1	00:04:17	192.168.1.2	stopped	00:00:07	
5	gi0/2	224.1.1.1	00:03:54	192.168.1.3	stopped	00:01:21	

#View the multicast forwarding table of Device 2.

```
Device2#show ip igmp snooping l3_ip_table
```

```
Total 1 entry
```

```
Flags: M - L2 multicast, S - short of resources
```

```
(*, 224.1.1.1)
```

```
Ingress Vlan: 2
```

```
Flags : M
```

```
L2 Interface List: gigabitethernet0/1
```

```
Egress Vlan  Flags  L3 Interface List
```

Egress Vlan	Flags	L3 Interface List
3	M	gigabitethernet0/3
4	M	gigabitethernet0/2
5	M	gigabitethernet0/2

#Multicast Server sends the multicast service packet with the destination address of 224.1.1.1. PC 1, PC 2 and PC 3 can correctly receive the multicast service packets.

## 66.3.2 Configure MVR

### Network Requirements

- On Device 1, configure the multicast routing protocol.

- There are 3 VLANs in the whole network, VLAN 2 to VLAN 4, and the port connected to the PC joins the corresponding VLAN in Hybrid mode.
- On Device 2, enable IGMP snooping and configure MVP.
- Multicast Server sends the multicast service packets, and PC 1, PC 2 and PC 3 can correctly receive the multicast service packets.

### Network Topology

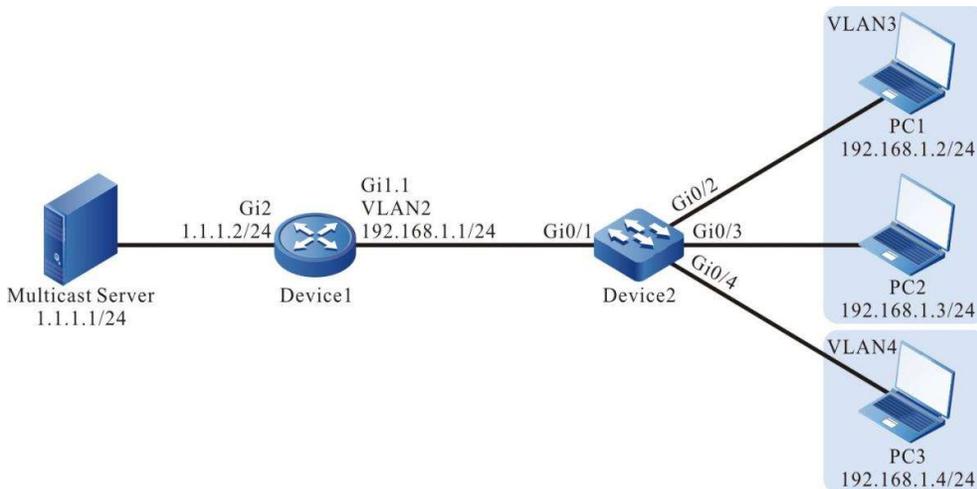


Figure 66-2 Network Topology for Configuring MVR

### Configuration Steps

Step 1: On Device 1, configure the interface IP address and enable the multicast routing protocol.  
(Omitted)

Step 2: Configure Device2.

#Create VLAN 2 to VLAN 4 on Device 2.

```
Device2#configure terminal
Device2(config)#vlan 2-4
```

#On Device 2, configure the link type of port gigabitethernet0/1 to Trunk to allow services of VLAN 2 to pass, and configure PVID to 1.

```
Device2(config)#interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#switchport mode hybrid
Device2(config-if-gigabitethernet0/1)#switchport hybrid tagged vlan 2
Device2(config-if-gigabitethernet0/1)# switchport hybrid pvid vlan 1
Device2(config-if-gigabitethernet0/1)#exit
```

#On Device 2, configure the link types of port gigabitethernet0/2-0/3 to Hybrid to allow services of VLAN 2 to VLAN 3 to pass, and configure PVID to 3.

```
Device2(config)#interface gigabitethernet 0/2-0/3
Device2(config-if-range)#switchport mode hybrid
Device2(config-if-range)#switchport hybrid untagged vlan 2-3
Device2(config-if-range)#switchport hybrid pvid vlan 3
Device2(config-if-range)#exit
```

#On Device 2, configure the link type of port gigabitethernet0/4 to Hybrid to allow services of VLAN 2 and VLAN 4 to pass, and configure PVID to 4.

```
Device2(config)#interface gigabitethernet 0/4
Device2(config-if-gigabitethernet0/4)#switchport mode hybrid
Device2(config-if-gigabitethernet0/4)#switchport hybrid untagged vlan 4
Device2(config-if-gigabitethernet0/4)#switchport hybrid untagged vlan 2
Device2(config-if-gigabitethernet0/4)#switchport hybrid pvid vlan 4
Device2(config-if-gigabitethernet0/4)#exit
```

#Configure IGMP Snooping.

```
Device2(config)#ip igmp snooping
Device2(config)#ip igmp snooping vlan 2
Device2(config)#ip igmp snooping vlan 3
Device2(config)#ip igmp snooping vlan 4
```

#Configure MVR.

```
Device2(config)#mvr vlan 2
Device2(config)#mvr enable
Device2(config)#exit
```

Step 3: Check the result.

#View MVR information.

```
Device2#show mvr
MVR status:enable
multicast-vlan: 2
```

#PC 1, PC 2 and PC 3 send IGMPv2 membership reports to join the multicast group 224.1.1.1.

#View the multicast membership table of Device 2.

```
Device2#show ip igmp snooping groups
IGMP Snooping Group Membership
Total 3 groups

VLAN ID Interface Name Group Address Expires Last Reporter V1 Expires V2 Expires Uptime
-----
2    gi0/2    224.1.1.1  00:04:14 192.168.1.2  stopped    00:00:07
```

2	gi0/3	224.1.1.1	00:04:14	192.168.1.3	stopped	00:00:07
2	gi0/4	224.1.1.1	00:04:14	192.168.1.4	stopped	00:00:07

It is indicated that all ports and groups are present in VLAN 2.

#Multicast Server sends the multicast service packet with the destination address of 224.1.1.1, and PC 1, PC 2 and PC 3 can correctly receive the multicast service packet.

# 67 IPv4 Multicast Basics

---

## 67.1 Overview

The IPv4 multicast basics section is the basics for running the IP multicast protocol and is a common part of all multicast protocols. To run any multicast routing protocol, you need to enable the IP multicast forwarding function before the device can forward multicast service packets.

## 67.2 IPv4 Multicast Basics Function Configuration

Table 67-1 IPv4 Multicast Basics Function Configuration List

Configuration Task	
Enable IP multicast forwarding	Enable IP multicast forwarding
Configure IP multicast forwarding rules	Configure multicast forwarding management boundaries
	Configure the limit of multicast forwarding entries

---

### Caution

- The L3 Ethernet interface does not support the function of IP multicast forwarding rules.
- 

### 67.2.1 Enable IP multicast forwarding

#### Configuration Condition

None

#### Enable IP multicast forwarding

Enabling the IP multicast forwarding function can ensure the normal operation of forwarding multicast services.

Table 67-2 Enabling IP Multicast Forwarding

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable IP multicast forwarding	<b>ip multicast-routing [ vrf vrf-name ]</b>	Mandatory  Enable IP multicast forwarding. By default, IP multicast forwarding is not enabled

## 67.2.2 Configure IP multicast forwarding rules

### Configuration Condition

Before configuring multicast forwarding management boundaries of the interface, do the following:

- Interface IP addresses have been configured so that neighbor nodes are reachable at the network layer.
- Enable IP multicast forwarding;
- Configure the multicast routing protocol.

### Configure multicast forwarding management boundaries

After the management boundaries are configured, the device can filter multicast service packets, and those that do not match the access list rules will not be forwarded through this interface.

Table 67-3 Configuring Multicast Forwarding Management Boundaries

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure multicast forwarding	<b>ip multicast boundary</b>	Mandatory

Step	Command	Description
management boundaries	{ <i>access-list-number</i>   <i>access-list-name</i> }	By default, no multicast forwarding management boundary is configured

### Configure the Timeout for Multicast Forwarding Entries

Configure the timeout for multicast forwarding entries, and delete or perform other operations according to the entry tags after the timeout.

Table 67-4 Configuring the Timeout for Multicast Forwarding Entries

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the Timeout for Multicast Forwarding Entries	<b>ip multicast mrt-timer</b> <i>timevalue</i>	Optional By default, the timeout for multicast forwarding entries is 180S

### Configure the limit of multicast forwarding entries

Configure the limit on the maximum number of the multicast forwarding entries. After the limit on the maximum number of the multicast forwarding entries is exceeded, newly added multicast forwarding entries will not be created.

Table 67-5 Configuring the Limit of Multicast Forwarding Entries

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the limit of multicast forwarding entries	<b>ip multicast route-limit</b> <i>number-value</i> [ <i>vrf vrf-name</i> ]	Optional By default, the maximum number of the multicast forwarding entries is 2047. The value range can be adjusted

Step	Command	Description
		according to the change of the system working mode

## Monitoring and Maintaining of IPv4 Multicast Basics

Table 67-6 Monitoring and Maintaining of IPv4 Multicast Basics

Command	Description
<b>clear ip mcache</b> [ <b>source</b> <i>source-ip-address</i> ] [ <b>group</b> <i>group-ip-address</i> ] [ <b>all</b>   <b>vrf</b> <i>vrf-name</i> ]	Clear multicast routing entries
<b>show ip mcache</b> [ <b>source</b> <i>source-ip-address</i> ] [ <b>group</b> <i>group-ip-address</i> ] [ <b>vrf</b> <i>vrf-name</i> ]	Show multicast routing table information
<b>show ip mnhp</b> [ [ <b>vrf</b> <i>vrf-name</i> ]   [ <b>vlan</b> <i>vlan-id</i> ] ]	Show multicast next hop information
<b>show ip mvif</b> [ <b>vrf</b> <i>vrf-name</i> ]	Show multicast virtual interface information
<b>show ip mvrf</b>	Show multicast VRF information

# 68 IGMP

---

## 68.1 Overview

IGMP (Internet Group Management Protocol) is a protocol responsible for IP multicast member management in the TCP/IP protocol family, which is used to establish and maintain multicast group membership between an IP host and multicast devices directly adjacent to it.

There are 3 versions of IGMP, and IGMPv2 is currently widely used. IGMPv2 has three types of packet: query packets, group membership reports, and group member leave packets.

Query packets include: general query packets and specified group query packets. The device learns which members are in the directly connected network via the general query packets, and learns whether there are members of a specified group in the directly connected network via the specified group query packets.

Group membership report: When the host wants to join one multicast group, it will immediately send a group membership report to the multicast group it wants to join. When the host receives one query packet, it also sends one group membership report.

Group member leave packet: When the host leaves one multicast group, it sends one group member leave report. When the device receives the group member leave packet, it sends one specified group query to determine whether the certain specific group has no members.

## 68.2 IGMP Function Configuration

Table 68-1 IGMP Function Configuration List

Configuration Task	
Configure basic IGMP functions	Enable IGMP protocol
	Configure IGMP version
	Configure static group joining
	Configure multicast group filter

Configuration Task	
	Configure SSM multicast group filter
Adjust and optimize IGMP network	Configure Query Interval of General Group
	Configure robustness variable
	Configure Max. Response Time
	Configure specified group query
	Configure the timeout of other queriers
	Configure Fast Leave

## Caution

- The L3 Ethernet interface does not support the IGMP function.

### 68.2.1 Configure basic IGMP functions

#### Configuration Condition

Before configuring the basic IGMP functions, do the following:

- Configure the network layer address of the interface so that all neighbor nodes are reachable at the network layer.

#### Enable IGMP protocol

Table 68-2 Enabling IGMP Protocol

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Enable IP multicast forwarding	<b>ip multicast-routing</b>	Mandatory By default, IP multicast forwarding is not enabled
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Enable IGMP protocol	<b>ip pim sparse-mode</b>	Mandatory By default, IGMP is not enabled. IGMP is automatically enabled when the multicast routing protocol is enabled on the interface. All IGMP-related configurations can only take effect after IGMP is enabled

### Configure IGMP version

Table 68-3 Configuring IGMP Version

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure IGMP version	<b>ip igmp version</b> <i>version-number</i>	Mandatory By default, the version of IGMP is 2

---

 **Note**

- Because the packet structures and types of different versions of IGMP protocol are different, it is recommended that all devices on the same subnet be configured with the same version of IGMP.
- 

### Configure static group joining

After the certain static group or source group is configured on the interface, the device considers that there are receivers of this multicast group or source group on the interface.

Table 68–4 Configuring Static Group Joining

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure static group joining	<b>ip igmp static-group</b> <i>group-ip-address</i> [ <i>source-ip-address</i> ]	Mandatory  By default, the interface does not statically join any multicast group or source group

### Configure multicast group filter

The interface configured with the IGMP multicast group filter will filter the group membership reports in that network segment according to the ACL rules. Only the group membership reports allowed by the ACL will be processed, and those that are not allowed will be dropped. For the existing multicast group that is not allowed by the ACL, the information of this multicast group will be deleted immediately.

Table 68–5 Configuring Multicast Group Filter

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-

Step	Command	Description
Configure IGMP multicast group filter	<b>ip igmp access-group</b> { <i>access-list-number</i>   <i>access-list-name</i> }	Mandatory  By default, no multicast group filter is configured

## Note

- The command **ip igmp access-group** only supports standard ACL.

### Configure SSM multicast group filter

After configuring the range of source groups accepted by IGMP, the received source group membership reports are filtered to limit the range of source groups served by the interface. For groups within the range of PIM-SSM, only IGMPv3 non-(IS\_EX, TO\_EX) membership reports of (S, G) allowed by the access list can be accepted.

Table 68–6 Configuring SSM Multicast Group Filter

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure SSM multicast group filter	<b>ip igmp ssm-access-group</b> { <i>access-list-number</i>   <i>access-list-name</i> }	Mandatory  By default, SSM group members are not limited for filtering

## Note

- The command **ip igmp ssm-access-group** takes effect only when IGMPv3 is enabled on the interface.

- 
- The command **ip igmp ssm-access-group** only takes effect for source groups within the range of PIM SSM.
  - The command **ip igmp access-group** only supports extended ACL.
- 

## 68.2.2 Adjust and optimize IGMP network

### Configuration Condition

Before adjusting and optimizing the IGMP network, do the following:

- Configure the network layer address of the interface so that all neighbor nodes are reachable at the network layer;
- Enable the IGMP protocol.

### Configure Query Interval of General Group

IGMP querier periodically sends the query packets of the general group to maintain the group member relation. You can modify the interval of sending the IGMP general group query packets according to the actuality of the network.

Table 68-7 Configuring Query Interval of General Group

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure Query Interval of General Group	<b>ip igmp query-interval</b> <i>interval-value</i>	Optional By default, the interval of sending the IGMP general group query packets is 125 seconds

---

### Note

- The value of the general query interval of the devices on the same network segment should
-

---

be kept as consistent as possible.

- The query interval of the general group should be larger than the maximum response time. Otherwise, the configuration cannot succeed.
- 

### Configure robustness variable

Table 68-8 Configuring Robustness Variable

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure robustness variable	<b>ip igmp robustness-variable</b> <i>variable-value</i>	Optional By default, the robustness variable of the IGMP querier is 2

---

### Note

- After configuring the robustness variable, the following parameters will also vary as the robustness parameter varies:
    - 1, group member timeout = robustness variable \* general group query time + maximum response time;
    - 2, other querier timeout = robustness variable \* general group query time + maximum response time / 2;
    - 3, it thus appears that the larger the value of the robustness variable, the longer the timeout of IGMP group members and the longer the timeout of other queriers. The user should set this value according to the actuality of the network.
- 

### Configure Max. Response Time

The general group query packet sent by the IGMPv2 querier contains the maximum response time field. The receiver sends the membership report packet within the maximum response interval.

Table 68-9 Configuring Maximum Response Time

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure Max. Response Time	<b>ip igmp query-max-response-time</b> <i>seconds</i>	Optional By default, the maximum response time for IGMP general group query is 10 seconds

### Configure specified group query

When the IGMP querier receives the leave packet of the certain multicast group, it sends the specified group query packet "specified group query count" times to query this segment for the multicast group, to learn whether the subnet has the members of the multicast group. If not receiving the membership report on the multicast group after waiting for "final lifecycle", delete the information of the multicast group.

Table 68-10 Configuring Specified Group Query

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure Query Interval of Specified Group	<b>ip igmp last-member-query-interval</b> <i>interval-value</i>	Optional By default, the interval of sending the specified group query packets is 1 second
Configure specified group query count	<b>ip igmp last-member-query-count</b> <i>count-value</i>	Optional By default, the count of sending

Step	Command	Description
		the specified group query packets is 2

## Note

- The command **ip igmp last-member-query-interval** and the command **ip igmp last-member-query-count** are invalid in the IGMPv1 version, because the IGMPv1 host will not send the leave packet when leaving the certain multicast group.

### Configure the timeout of other queriers

In the same subnet, the device with a smaller address is elected as the querier, and other devices are called non-queriers. On non-queriers, the querier will be set a timer (there is a timer for each other querier) having a timeout of 'other querier timeout'. When the non-querier receives the query packet from the querier, this timer will be refreshed. When the timer expires, it means that the current IGMP querier has expired and a new one must be re-elected.

Table 68-11 Configuring the Timeout of Other Queriers

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure the timeout of other queriers	<b>ip igmp query-timeout</b> <i>seconds</i>	Optional By default, the timeout of other queriers is 255 seconds

## Caution

- If the configured timeout of other queriers is less than the query interval, the querier in the

---

network may change repeatedly.

---

### Configure Fast Leave

Only one host is connected to the stub segment of the network to frequently switch the multicast groups. To reduce the leave delay, you can configure the multicast group fast leave on the device.

If the device receives the leave packet of one multicast group after configuring fast leave, the device checks whether the multicast group is within the fast leave range. If yes, the device does not send the specified group query packet within the network segment any more and the information of the multicast group is deleted at once.

Table 68-11 Configuring Fast Leave

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure the range of fast leave from the multicast group	<b>ip igmp immediate-leave group-list</b> { <i>access-list-number</i>   <i>access-list-name</i> }	Mandatory  By default, fast leave from the multicast group is not allowed, and this is applicable to IGMPv2
Configure the range of fast leave from the source group	<b>ip igmp sg-immediate-leave sg-list</b> { <i>access-list-number</i>   <i>access-list-name</i> }	Mandatory  By default, fast leave from the source group is not allowed, and this is applicable to IGMPv3

### 68.2.3 Configure IGMP SSM Mapping

#### Configuration Condition

Before configuring IGMP SSM Mapping, do the following:

- Configure the network layer address of the interface so that all neighbor nodes are reachable at the network layer.
- Enable the IGMP protocol.

### Configure IGMP SSM Mapping

In order to provide PIM-SSM services to receivers who do not support IGMPv3 in the PIM-SSM network, you can configure the IGMP SSM mapping function on the device.

The user can configure IGMP SSM mapping rules according to the needs of the network receivers. The group membership reports allowed by the rules are converted into IGMPv3 non-(IS\_EX, TO\_EX) membership reports, and the multicast source address is the source address specified by the IGMP SSM mapping rules.

Table 68-12 Configuring IGMP SSM Mapping

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable IGMP SSM Mapping	<b>ip igmp ssm-map enable [ vrf vrf-name ]</b>	Mandatory By default, IGMP SSM Mapping is not enabled
Configure IGMP SSM Mapping rules	<b>ip igmp ssm-map static</b> <i>{ access-list-number   access-list-name }</i> <i>source-ip-address [ vrf vrf-name ]</i>	Mandatory By default, there is no IGMP SSM Mapping rule

### Note

- The command `ip igmp ssm-map static` only supports standard ACL.

## 68.2.4 IGMP Monitoring and Maintaining

Table 68-13 IGMP Monitoring and Maintaining

Command	Description
<b>clear ip igmp group</b> [ <i>group-ip-address</i> ] [ <i>interface-name</i> ] [ <i>vrf vrf-name</i> ]	Clear IGMP multicast group information
<b>clear ip igmp statistic interface</b> <i>interface-name</i> [ <i>vrf vrf-name</i> ]	Clear IGMP packet statistics on the interface
<b>show ip igmp groups</b> [ [ <i>static</i> ]   [ <i>interface-name</i> ] [ <i>group-ip-address</i> ] [ <i>detail</i> ] ] [ <i>vrf vrf-name</i> ]	Show IGMP multicast group information
<b>show ip igmp interface</b> [ <i>interface-name</i> ] [ <i>vrf vrf-name</i> ]	Show interface IGMP information
<b>show ip igmp statistic interface</b> <i>interface-name</i> [ <i>vrf vrf-name</i> ]	Show statistics of IGMP packets

## 68.3 IGMP Typical Configuration Example

### 68.3.1 Configure IGMP

#### Network Requirements

- The PIM-SM protocol runs on the entire network.
- Device 1, Device 2, and Receiver are in the same LAN, and Device 2 is the querier.
- Receiver is one receiver of the Device 1 and Device 2 stub network.
- IGMPv2 runs between Device 1 and 2 and the stub network.

#### Network Topology

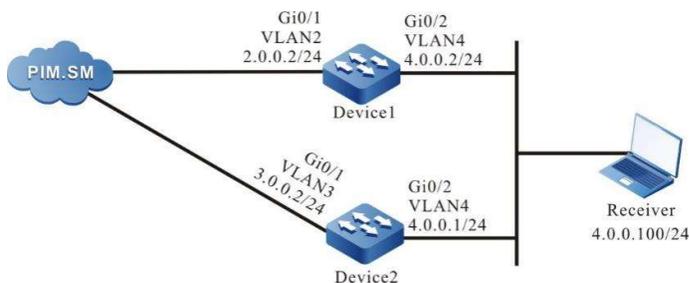


Figure 68-1 Network Topology for Configuring IGMP

#### Configuration Steps

Step 1: Configure IP addresses for the ports. (Omitted)

Step 2: Enable multicast forwarding globally, and enable the multicast protocol PIM-SM on the interfaces.

#Configure Device1.

Enable multicast forwarding globally, and enable the multicast protocol PIM-SM on related interfaces.

```
Device1(config)#configure terminal
Device1(config)#ip multicast-routing
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ip pim sparse-mode
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan4
Device1(config-if-vlan4)#ip pim sparse-mode
Device1(config-if-vlan4)#exit
```

#Configure Device2.

Enable multicast forwarding globally, and enable the multicast protocol PIM-SM on related interfaces.

```
Device2(config)#configure terminal
Device2(config)#ip multicast-routing
Device2(config)#interface vlan3
Device2(config-if-vlan3)#ip pim sparse-mode
Device2(config-if-vlan3)#exit
Device2(config)#interface vlan4
Device2(config-if-vlan4)#ip pim sparse-mode
Device2(config-if-vlan4)#exit
```

Step 3: Check the result.

#View the IGMP version information and querier election result of Device 1 interface vlan 4.

```
Device1#show ip igmp interface vlan4
Interface vlan4 (Index 50331921)
IGMP Active, Non-Querier (4.0.0.1, Expires: 00:02:15)
Default version 2
IP router alert option in IGMP V2 msgs: EXCLUDE
Internet address is 4.0.0.2
IGMP query interval is 125 seconds
IGMP querier timeout is 255 seconds
IGMP max query response time is 10 seconds configged, and 10 seconds is adopted
```

Last member query response interval is 1 seconds  
Last member query count is 2  
Group Membership interval is 260 seconds  
IGMP robustness variable is 2

#### #View the IGMP version information and querier election result of Device 2 interface vlan 4.

```
Device2#show ip igmp interface vlan4
Interface vlan4 (Index 50331921)
IGMP Active, Querier (4.0.0.1)
Default version 2

IP router alert option in IGMP V2 msgs: EXCLUDE
Internet address is 4.0.0.1
IGMP query interval is 125 seconds
IGMP querier timeout is 255 seconds
IGMP max query response time is 10 seconds
Last member query response interval is 1 seconds
Last member query count is 2
Group Membership interval is 260 seconds
IGMP robustness variable is 2
```

#### #Receiver sends an IGMPv2 membership report to join the multicast group 225.1.1.1.

#### #View the multicast membership table of Device 1.

```
Device1#show ip igmp groups
IGMP Connected Group Membership
Total 1 groups
Group Address  Interface      Uptime   Expires  Last Reporter  V1 Expires  V2 Expires
225.1.1.1     vlan4          00:21:02 00:03:47 4.0.0.100     stopped
```

#### #View the multicast membership table of Device 2.

```
Device2#show ip igmp groups
IGMP Connected Group Membership
Total 1 groups
Group Address  Interface      Uptime   Expires  Last Reporter  V1 Expires  V2 Expires
225.1.1.1     vlan4          00:21:02 00:03:47 4.0.0.100     stopped
```

---

### Note

- After the multicast protocol is configured on the interface, the IGMP function is automatically enabled, and the IGMPv2 version is run by default. By the command **ip igmp version** you can configure the IGMP version that runs on the interface.
- When multiple devices in the same LAN run IGMP, the election of IGMP queriers will be

---

performed, and one with the smaller IP address is elected as the IGMP querier of this LAN.

---

## 68.3.2 Configure IGMP SSM Mapping

### Network Requirements

- The PIM-SSM protocol runs on the entire network.
- Receiver 1, Receiver 2, Receiver 3, and Device 2 are in the same LAN.
- IGMPv3 runs between Device 2 and the stub network.
- By using IGMP SSM mapping on Device 2, Receiver 2 and Receiver 3 can only receive multicast packets sent by Source 1.

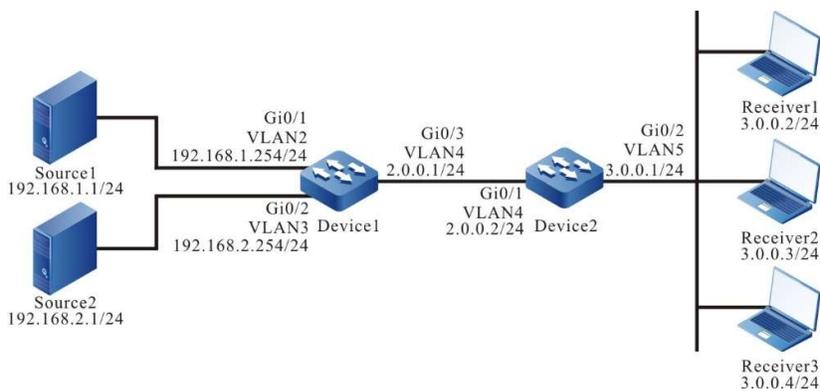


Figure 68-2 Network Topology for Configuring IGMP SSM Mapping

### Configuration Steps

Step 1: Configure IP addresses for the interfaces (omitted).

Step 2: Enable the unicast routing protocol OSPF, so that all network devices in the network can communicate with each other.

#### #Configure Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 192.168.1.0 0.0.0.255 area 0
Device1(config-ospf)#network 192.168.2.0 0.0.0.255 area 0
Device1(config-ospf)#exit
```

#### #Configure Device2.

```
Device2#configure terminal
```

```
Device2(config)#router ospf 100
Device2(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#exit
```

### #View the routing table of Device 2.

```
Device2#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS
```

```
Gateway of last resort is not set
```

```
C 2.0.0.0/24 is directly connected, 00:16:05, vlan4
C 3.0.0.0/24 is directly connected, 00:06:36, vlan5
O 192.168.1.0/24 [110/2] via 2.0.0.1, 00:15:17, vlan4
O 192.168.2.0/24 [110/2] via 2.0.0.1, 00:00:51, vlan4
```

---

## Note

- Device 1 is viewed the same way as Device 2, and the viewing process is omitted.
- 

Step 3: Enable multicast forwarding globally, and configure PIM-SSM globally. The range of multicast groups served by SSM is 232.0.0.0/8. Enable the multicast protocol PIM-SM on the interfaces. IGMPv3 runs on the interface vlan 5 of Device 2.

### #Configure Device1.

Enable multicast forwarding globally, configure PIM-SSM globally, and enable the multicast protocol PIM-SM on related interfaces.

```
Device1(config)#ip multicast-routing
Device1(config)#ip pim ssm default
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ip pim sparse-mode
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan3
Device1(config-if-vlan3)#ip pim sparse-mode
Device1(config-if-vlan3)#exit
Device1(config)#interface vlan4
Device1(config-if-vlan4)#ip pim sparse-mode
Device1(config-if-vlan4)#exit
```

#Configure Device2.

Enable multicast forwarding globally, configure PIM-SSM globally, and enable the multicast protocol PIM-SSM on related interfaces, with IGMPv3 running on the interface vlan 5.

```
Device2(config)#ip multicast-routing
Device2(config)#ip pim ssm default
Device2(config)#interface vlan4
Device2(config-if-vlan4)#ip pim sparse-mode
Device2(config-if-vlan4)#exit
Device2(config)#interface vlan5
Device2(config-if-vlan5)#ip pim sparse-mode
Device2(config-if-vlan5)#ip igmp version 3
Device2(config-if-vlan5)#exit
```

#View the IGMP information of the interface vlan 5 of Device 2.

```
Device2#show ip igmp interface vlan5
Interface vlan5 (Index 50331921)
IGMP Enabled, Active, Querier (3.0.0.1)
Configured for version 3
IP router alert option in IGMP V2 msgs: EXCLUDE
Internet address is 3.0.0.1
IGMP query interval is 125 seconds
IGMP querier timeout is 255 seconds
IGMP max query response time is 10 seconds
Last member query response interval is 1 seconds
Last member query count is 2
Group Membership interval is 260 seconds
IGMP robustness variable is 2
```

Step 4: Enable IGMP SSM mapping on Device 2 and configure IGMP SSM mapping rules so that Receiver 1 and Receiver 2 can only receive multicast packets sent by Source 1.

#Configure Device2.

Enable IGMP SSM mapping, configure the multicast group range for IGMP SSM mapping to 232.0.0.0-232.0.0.255, with the multicast source address of 192.168.1.1.

```
Device2(config)#ip access-list standard 1
Device2(config-std-nacl)#permit 232.0.0.0 0.255.255.255
Device2(config-std-nacl)#commit
Device2(config-std-nacl)#exit
Device2(config)#ip igmp ssm-map enable
Device2(config)#ip igmp ssm-map static 1 192.168.1.1
```

#View the IGMP SSM mapping rules of Device 2.

```
Device2#show ip igmp ssm-map

IGMP SSM-MAP Information : enable

acl-name source-addr
-----
1      192.168.1.1
```

Step 5: Check the result.

#Receiver 1 sends the IGMPv3 membership report of the specified source group to join the multicast group 232.1.1.1, with the specified multicast source of 192.168.2.1; Receiver 2 sends the IGMPv2 membership report to join the multicast group 232.1.1.2; Receiver 3 sends the IGMPv1 membership report to join the multicast group 232.1.1.3.

#Both Source 1 and Source 2 send the multicast packets of the multicast groups 232.1.1.1, 232.1.1.2, and 232.1.1.3.

#View the multicast membership table of Device 2.

```
Device2#show ip igmp groups

IGMP Connected Group Membership

Total 3 groups

Group Address  Interface    Uptime  Expires  Last Reporter  V1 Expires  V2 Expires
232.1.1.1     vlan5       01:28:45  stopped  3.0.0.2        stopped     stopped
232.1.1.2     vlan5       01:29:01  stopped  3.0.0.3        stopped     stopped
232.1.1.3     vlan5       01:29:16  stopped  3.0.0.4        stopped     stopped
```

```
Device2#show ip igmp groups detail

Interface:vlan5

Group:      232.1.1.1
Uptime:    01:30:44
Group mode: Include
Last reporter: 3.0.0.2
TIB-A Count: 1
TIB-B Count: 0
Group source list: (R - Remote, M - SSM Mapping)

Source Address  Uptime  v3 Exp  M Exp  Fwd  Flags
192.168.2.1    01:30:44  00:03:39  stopped  Yes  R
```

```
Interface: vlan5

Group:      232.1.1.2
Uptime:    01:31:00
```

Group mode: Include  
Last reporter: 3.0.0.3  
TIB-A Count: 1  
TIB-B Count: 0  
Group source list: (R - Remote, M - SSM Mapping)  
Source Address Uptime v3 Exp M Exp Fwd Flags  
192.168.1.1 01:31:00 stopped 00:03:38 Yes M

Interface: vlan5  
Group: 232.1.1.3  
Uptime: 01:31:15  
Group mode: Include  
Last reporter: 3.0.0.4  
TIB-A Count: 1  
TIB-B Count: 0  
Group source list: (R - Remote, M - SSM Mapping)  
Source Address Uptime v3 Exp M Exp Fwd Flags  
192.168.1.1 01:31:15 stopped 00:03:42 Yes M

#### #View the multicast routing table of Device 2.

```
Device2#show ip pim mroute
IP Multicast Routing Table:
PIM VRF Name: Default
Total 0 (*,*,RP) entry
Total 0 (*,G) entry
Total 3 (S,G) entries
Total 0 (S,G,rpt) entry
Total 0 FCR entry
Up timer/Expiry timer
```

```
(192.168.2.1, 232.1.1.1)
Up time: 01:32:51
KAT time: 00:03:24
RPF nbr: 2.0.0.1
RPF idx: vlan4
SPT bit: TRUE
Flags:
JOIN DESIRED
Upstream State: JOINED
Local interface list:
```

Vlan5  
Joined interface list:  
Asserted interface list:  
**Outgoing interface list:**  
    Vlan5  
Packet count 19868613

(192.168.1.1, 232.1.1.2)

Up time: 01:33:07  
KAT time: 00:03:24  
RPF nbr: 2.0.0.1  
RPF idx: vlan4  
SPT bit: TRUE  
Flags:  
    JOIN DESIRED  
Upstream State: JOINED

Local interface list:  
    Vlan5  
Joined interface list:  
Asserted interface list:  
**Outgoing interface list:**  
    Vlan5  
Packet count 19873645

(192.168.1.1, 232.1.1.3)

Up time: 01:33:22  
KAT time: 00:03:24  
RPF nbr: 2.0.0.1  
RPF idx: vlan4  
SPT bit: TRUE  
Flags:  
    JOIN DESIRED  
Upstream State: JOINED

Local interface list:  
    Vlan5  
Joined interface list:  
Asserted interface list:  
**Outgoing interface list:**  
    Vlan5  
Packet count 19873645

#Receiver 1 can only receive multicast packets sent by Source 2, and Receiver 2 and Receiver 3 can only receive multicast packets sent by Source 1.

---

## Note

- Device 1 is viewed the same way as Device 2, and the viewing process is omitted.
  - IGMP SSM mapping needs to be used in conjunction with PIM-SSM. The multicast group range in the IGMP SSM mapping rules must be within the multicast group range of PIM-SSM. IGMP SSM mapping mainly provides support for the SSM model for the receiver host that runs IGMPv1 or IGMPv2 and cannot be upgraded to IGMPv3.
  - IGMP SSM mapping is invalid to IGMPv3 membership reports.
- 

### 68.3.3 Configure IGMP Static Group Joining

#### Network Requirements

- The PIM-SM protocol runs on the entire network.
- Receiver is one receiver of Device stub network.
- IGMPv2 runs between Device and the stub network.
- The interface vlan 3 of Device joins the multicast group 225.1.1.1 in a static joining manner.

#### Network Topology



Figure 68-3 Network Topology for Configuring IGMP Static Group Joining

#### Configuration Steps

Step 1: Configure IP addresses for the ports. (Omitted)

Step 2: Enable multicast forwarding globally, and enable the multicast protocol PIM-SM on the interfaces.

#Configure Device.

Enable multicast forwarding globally, and enable the multicast protocol PIM-SM on related interfaces.

```
Device(config)#configure terminal
Device(config)#ip multicast-routing
Device(config)#interface vlan2
Device(config-if-vlan2)#ip pim sparse-mode
Device(config-if-vlan2)#exit
Device(config)#interface vlan3
Device(config-if-vlan3)#ip pim sparse-mode
Device(config-if-vlan3)#exit
```

#View the IGMP information of the interface vlan 3 of Device.

```
Device#show ip igmp interface vlan3
Interface vlan3 (Index 50331921)
IGMP Active, Querier (3.0.0.1)
Default version 2
IP router alert option in IGMP V2 msgs: EXCLUDE
Internet address is 3.0.0.1
IGMP query interval is 125 seconds
IGMP querier timeout is 255 seconds
IGMP max query response time is 10 seconds
Last member query response interval is 1 seconds
Last member query count is 2
Group Membership interval is 260 seconds
IGMP robustness variable is 2
```

Step 3: The interface vlan 3 of Device joins the multicast group 225.1.1.1 in a static joining manner.

#Configure Device.

Configure the static multicast group 225.1.1.1 on the interface vlan 3 of Device.

```
Device(config)#interface vlan3
Device(config-if-vlan3)#ip igmp static-group 225.1.1.1
Device(config-if-vlan3)#exit
```

Step 4: Check the result.

#Source sends the multicast packet of the multicast group 225.1.1.1.

#View the multicast membership table of Device.

```
Device#show ip igmp groups
IGMP Static Group Membership
```

Total 1 static groups

Group Address	Source Address	Interface
225.1.1.1	0.0.0.0	vlan3

#View the multicast routing table of Device.

Device#show ip pim mroute

IP Multicast Routing Table:

PIM VRF Name: Default

Total 0 (\*,\*,RP) entry

Total 1 (\*,G) entry

Total 1 (S,G) entry

Total 1 (S,G,rpt) entry

Total 0 FCR entry

Up timer/Expiry timer

(\*, 225.1.1.1)

Up time: 00:08:12

RP: 0.0.0.0

RPF nbr: 0.0.0.0

RPF idx: None

Flags:

JOIN DESIRED

Upstream State: JOINED

Local interface list:

vlan3

Joined interface list:

Asserted interface list:

(192.168.1.1, 225.1.1.1)

Up time: 00:07:24

KAT time: 00:02:22

RPF nbr: 0.0.0.0

RPF idx: None

SPT bit: TRUE

Flags:

JOIN DESIRED

COULD REGISTER

Upstream State: JOINED

Local interface list:

```

Joined interface list:
  register_vif0
Asserted interface list:
Outgoing interface list:
  register_vif0
  vlan3
Packet count 8646421

(192.168.1.1, 225.1.1.1, rpt)
Up time: 00:07:24
RP: 0.0.0.0
Flags:
  RPT JOIN DESIRED
  RPF SGRPT XG EQUAL
Upstream State: NOT PRUNED
Local interface list:
Pruned interface list:
Outgoing interface list:
  vlan3

```

#Receiver can receive the multicast packet of the multicast group 225.1.1.1 sent by Source.

### 68.3.4 Configure IGMP Multicast Group Filtering

#### Network Requirements

- The PIM-SM protocol runs on the entire network.
- Receiver is one receiver of Device stub network.
- IGMPv2 runs between Device and the stub network.
- The interface vlan 3 of Device filters the multicast groups, and the range of multicast groups that Receiver is allowed to join is 225.1.1.0-225.1.1.255.

#### Network Topology

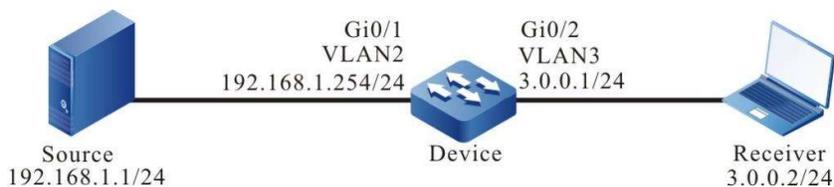


Figure 68-4 Network Topology for Configuring IGMP Multicast Group Filtering

## Configuration Steps

Step 1: Configure IP addresses for the ports. (Omitted)

Step 2: Enable multicast forwarding globally, and enable the multicast protocol PIM-SM on the interfaces.

#Configure Device.

Enable multicast forwarding globally, and enable the multicast protocol PIM-SM on related interfaces.

```
Device(config)#configure terminal
Device(config)#ip multicast-routing
Device(config)#interface vlan2
Device(config-if-vlan2)#ip pim sparse-mode
Device(config-if-vlan2)#exit
Device(config)#interface vlan3
Device(config-if-vlan3)#ip pim sparse-mode
Device(config-if-vlan3)#exit
```

#View the IGMP information of the interface vlan 3 of Device.

```
Device#show ip igmp interface vlan3
Interface vlan3 (Index 50331921)
IGMP Enabled, Active, Querier (3.0.0.1)
Default version 2
IP router alert option in IGMP V2 msgs: EXCLUDE
Internet address is 3.0.0.1
IGMP query interval is 125 seconds
IGMP querier timeout is 255 seconds
IGMP max query response time is 10 seconds
Last member query response interval is 1 seconds
Last member query count is 2
Group Membership interval is 260 seconds
IGMP robustness variable is 2
```

Step 3: Configure multicast group filtering on the interface vlan 3 of Device.

#Configure Device.

Configure multicast group filtering on the interface vlan 3 of Device, with the range of multicast groups that Receiver is allowed to join being 225.1.1.0-225.1.1.255.

```

Device(config)#ip access-list standard 1
Device(config-std-nacl)#permit 225.1.1.0 0.0.0.255
Device(config-std-nacl)#commit
Device(config-std-nacl)#exit
Device(config)#interface vlan3
Device(config-if-vlan3)#ip igmp access-group 1
Device(config-if-vlan3)#exit

```

Step 4: Check the result.

#Receiver sends an IGMPv2 leave packet to join the multicast groups 225.1.1.1. and 226.1.1.1.

#Source sends the multicast packet of the multicast groups 225.1.1.1 and 226.1.1.1.

#View the multicast membership table of Device.

```

Device#show ip igmp groups
IGMP Connected Group Membership
Total 1 groups

```

Group Address	Interface	Uptime	Expires	Last Reporter	V1 Expires	V2 Expires
225.1.1.1	vlan3	03:14:59	00:03:05	3.0.0.2	stopped	

#View the multicast routing table of Device.

```

Device#show ip pim mroute
IP Multicast Routing Table:
PIM VRF Name: Default
Total 0 (*,*,RP) entry
Total 1 (*,G) entry
Total 2 (S,G) entries
Total 2 (S,G,rpt) entries
Total 0 FCR entry
Up timer/Expiry timer

```

(\*, 225.1.1.1)

Up time: 00:00:56

RP: 0.0.0.0

RPF nbr: 0.0.0.0

RPF idx: None

Flags:

JOIN DESIRED

Upstream State: JOINED

Local interface list:

vlan3

Joined interface list:

Asserted interface list:

(192.168.1.1, 225.1.1.1)

Up time: 00:00:15

KAT time: 00:03:15

RPF nbr: 0.0.0.0

RPF idx: None

SPT bit: TRUE

Flags:

JOIN DESIRED

COULD REGISTER

Upstream State: JOINED

Local interface list:

Joined interface list:

register\_vif0

Asserted interface list:

Outgoing interface list:

register\_vif0

vlan3

Packet count 1

(192.168.1.1, 225.1.1.1, rpt)

Up time: 00:00:15

RP: 0.0.0.0

Flags:

RPT JOIN DESIRED

RPF SGRPT XG EQUAL

Upstream State: NOT PRUNED

Local interface list:

Pruned interface list:

Outgoing interface list:

vlan3

(192.168.1.1, 226.1.1.1)

Up time: 00:00:15

KAT time: 00:03:15

RPF nbr: 0.0.0.0

RPF idx: None

SPT bit: TRUE

Flags:

JOIN DESIRED

COULD REGISTER

Upstream State: JOINED

Local interface list:

Joined interface list:

register\_vif0

Asserted interface list:

Outgoing interface list:

register\_vif0

Packet count 1

(192.168.1.1, 226.1.1.1, rpt)

Up time: 00:00:15

RP: 0.0.0.0

Flags:

RPF SGRPT XG EQUAL

Upstream State: RPT NOT JOINED

Local interface list:

Pruned interface list:

Outgoing interface list:

#Receiver can only receive the multicast packet of the multicast group 225.1.1.1 sent by Source.

---

## Note

- If you want to filter based on the multicast source group, you can use the command **ip igmp ssm-access-group** to achieve this. When using this command, the device is required to run PIM-SSM and the interface to run IGMPv3 version.
-

# 69 PIM-DM

---

## 69.1 Overview

PIM-DM (Protocol Independent Multicast-Dense Mode) is mainly applicable to the cases where the distribution of group members is relatively concentrated and the range is small, or the network bandwidth resources are abundant.

PIM-DM is independent of the specific unicast routing protocol for RPF inspection.

PIM-DM uses "Push" to transmit the multicast data packets. When the multicast source starts to send the multicast data packets, it is assumed that all subnets in the multicast domain have multicast receivers, so the multicast data packets will be pushed to all nodes in the network. PIM-DM will prune the multicast forwarding branches without receivers. When the receiver of the multicast source appears on the node of the pruned multicast forwarding branch, PIM-DM uses the grafting mechanism to actively resume the forwarding of multicast data.

PIM-DM uses a status refresh mechanism to periodically refresh the downstream status so that the pruned branch will not time out.

## 69.2 PIM-DM Function Configuration

Table 69-1 PIM-DM Function Configuration List

Configuration Task	
Configure basic functions of PIM-DM	Configure PIM-DM protocol
Configure PIM-DM neighbors	Configure sending period of HELLO packets
	Configure PIM-DM neighbor keepalive time

Configuration Task	
	Configure PIM-DM neighbor filtering
Configure state refresh parameters	Configure PIM-DM state refresh interval

## Caution

- The L3 Ethernet interface does not support the PIM-DM function.

### 69.2.1 Configure basic functions of PIM-DM

#### Configuration Condition

Before configuring PIM-DM, do the following:

- Configure the network layer address of the interface so that all neighbor nodes are reachable at the network layer;
- Configure any unicast routing protocol to achieve reachable routes within the domain;
- Enable IP multicast forwarding function.

#### Configure PIM-DM protocol

Table 69-2 Configuring PIM-DM Protocol

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-

Step	Command	Description
Enable PIM-DM protocol	<b>ip pim dense-mode</b>	Either-or
	<b>ip pim dense-mode passive</b>	By default, the interface is in PIM-DM disabled status  The command <b>ip pim dense-mode passive</b> enables the PIM-DM protocol, and the interface does not send the hello packet to neighbors

## 69.2.2 Configure PIM-DM neighbors

### Configuration Condition

Before configuring PIM-DM neighbors, do the following:

- Configure the network layer address of the interface so that all neighbor nodes are reachable at the network layer;
- Configure any unicast routing protocol to achieve reachable routes within the domain;
- Enable the PIM-DM protocol.

### Configure sending period of HELLO packets

The interface with the PIM-DM protocol enabled will periodically send the Hello packet to establish and maintain PIM-DM neighbors.

Table 69-3 Configuring Sending Period of HELLO Packets

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface	<b>interface <i>interface-name</i></b>	-

Step	Command	Description
configuration mode		
Configure sending period of HELLO packets	<b>ip pim dense-mode hello-interval</b> <i>interval-value</i>	Optional By default, the interval of sending the Hello packet is 30 seconds

### Configure PIM-DM neighbor keepalive time

When the Hello packet from one neighbor is received on the interface, the holdtime carried in the Hello packet will be recorded as the keepalive time of this neighbor. If no Hello packet of the neighbor is received within the keep-alive period, this neighbor is considered invalid.

Table 69-4 Configuring PIM-DM Neighbor Keepalive Time

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure PIM-DM neighbor keepalive time	<b>ip pim dense-mode hello-holdtime</b> <i>holdtime-value</i>	Optional By default, the keepalive time of a PIM-DM neighbor is 105 seconds

### Configure PIM-DM neighbor filtering

To save system resources, you can use the neighbor filtering function to selectively establish neighbors, thereby saving device resources.

Table 69-5 Configuring PIM-DM Neighbor Filtering

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure PIM-DM neighbor filtering	<b>ip pim dense-mode neighbor-filter</b> { <i>access-list-number</i>   <i>access-list-name</i> }	Optional By default, the PIM-DM neighbor filtering function is not enabled

### 69.2.3 Configure state refresh parameters

#### Configuration Condition

Before configuring PIM-DM state refresh parameters, do the following:

- Configure the network layer address of the interface so that all neighbor nodes are reachable at the network layer;
- Configure any unicast routing protocol to achieve reachable routes within the domain;
- Enable the PIM-DM protocol.

#### Configure PIM-DM state refresh interval

For PIM-DM, it is required to set the interval for the router directly connected to the source to generate the status refresh packet.

Table 69-6 Configuring PIM-DM State Refresh Interval

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure PIM-DM state refresh interval	<b>ip pim dense-mode state-refresh origination-interval</b> <i>interval-value</i>	Optional By default, the PIM-DM state refresh interval is 60 seconds

## 69.2.4 PIM-DM Monitoring and Maintaining

Table 69-7 PIM-DM Monitoring and Maintaining

Command	Description
<b>clear ip pim dense-mode mroute</b> [ <i>group-ip-address source-ip-address</i> ] [ <b>vrf</b> <i>vrf-name</i> ]	Clear PIM-DM multicast routing information
<b>show ip pim dense-mode interface</b> [ <b>detail</b> ] [ <b>vrf</b> <i>vrf-name</i> ]	Show PIM-DM interface information
<b>show ip pim dense-mode neighbor</b> [ <b>detail</b> ] [ <b>vrf</b> <i>vrf-name</i> ]	Show PIM-DM neighbor information
<b>show ip pim dense-mode nexthop</b> [ <i>source-ip-address</i> ] [ <b>vrf</b> <i>vrf-name</i> ]	Show the unicast next hop information from PIM-DM to the source
<b>show ip pim dense-mode mroute</b> [ [ <b>group</b> <i>group-ip-address</i> ] [ <b>source</b> <i>source-ip-address</i> ] ]	Show the routing table information for the PIM-DM protocol

Command	Description
[ <b>source</b> <i>source-ip-address</i> <b>group</b> <i>group-ip-address</i> ] [ <b>vrf</b> <i>vrf-name</i> ]	

## 69.3 PIM-DM Typical Configuration Example

### 69.3.1 Configure basic functions of PIM-DM

#### Network Requirements

- Enable the PIM-DM protocol on the entire network.
- Receiver is one receiver of Device 2 stub network.
- IGMPv2 runs between Device 2 and the stub network.

#### Network Topology

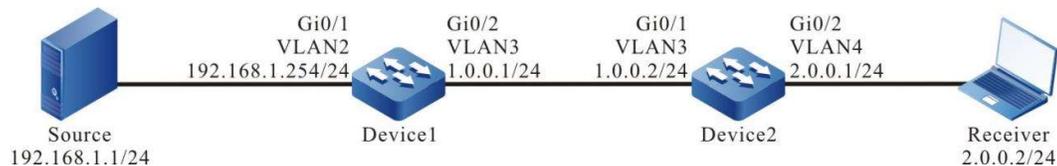


Figure 69-1 Network Topology for Configuring Basic Functions of PIM-DM

#### Configuration Steps

- Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)
- Step 2: Configure IP addresses for the ports. (Omitted)
- Step 3: Enable the unicast routing protocol OSPF, so that all devices in the network can communicate with each other.

#### #Configure Device1.

```

Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#network 1.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 192.168.1.0 0.0.0.255 area 0
Device1(config-ospf)#exit
  
```

## #Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 1.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#exit
```

## #View the routing table of Device 2.

```
Device2#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, Ex - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C 1.0.0.0/24 is directly connected, 00:07:30, vlan3
C 2.0.0.0/24 is directly connected, 00:07:14, vlan4
O 192.168.1.0/24 [110/2] via 1.0.0.1, 00:00:16, vlan3
```

---

### Note

- The routing table of Device 1 is viewed the same way as that of Device 2.
- 

Step 4: Enable multicast forwarding globally, and enable the multicast protocol PIM-DM on the interfaces.

## #Configure Device1.

Enable multicast forwarding globally, and enable the multicast protocol PIM-DM on related interfaces.

```
Device1(config)#ip multicast-routing
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#ip pim dense-mode
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan 3
Device1(config-if-vlan3)#ip pim dense-mode
Device1(config-if-vlan3)#exit
```

## #Configure Device2.

Enable multicast forwarding globally, and enable the multicast protocol PIM-DM on related interfaces.

```
Device2(config)#ip multicast-routing
Device2(config)#interface vlan 3
Device2(config-if-vlan3)#ip pim dense-mode
Device2(config-if-vlan3)#exit
Device2(config)#interface vlan 4
Device2(config-if-vlan4)#ip pim dense-mode
Device2(config-if-vlan4)#exit
```

#View, for Device 2, interface information with PIM-DM protocol enabled and PIM-DM neighbor information.

```
Device2#show ip pim dense-mode interface
Total 2 Interface entries
Total 0 External Interface entry
Total 0 Sparse-Dense Mode Interface entry
Address      Interface    VIFIndex Ver/  Nbr  VIF
              Mode    Count Flag
1.0.0.2     vlan3        0   v2/D  1   UP
2.0.0.1     vlan4        1   v2/D  0   UP

Device2#show ip pim dense-mode neighbor
PIM Dense-mode Neighbor Table:
PIM Dense-mode VRF Name: Default
Total 1 Neighbor entries

Neighbor-Address Interface    Uptime/Expires  Ver
1.0.0.1     vlan3        00:02:15/00:01:30 v2
```

#View the IGMP information of the interface VLAN 4 of Device 2.

```
Device2#show ip igmp interface vlan 4
Interface vlan4 (Index 65547)
IGMP Active, Querier (2.0.0.1)
Default version 2
IP router alert option in IGMP V2 msgs: EXCLUDE
Internet address is 2.0.0.1
IGMP query interval is 125 seconds
IGMP querier timeout is 255 seconds
IGMP max query response time is 10 seconds
Last member query response interval is 1 seconds
```

Last member query count is 2  
Group Membership interval is 260 seconds  
IGMP robustness variable is 2

---

## Note

- Information of Device 1 is viewed the same way as that of Device 2.
  - After the multicast protocol is configured on the interface, the IGMP function is automatically enabled, and IGMPv2 is run by default. By executing the command **ip igmp version** you can configure the IGMP version that runs on the interface.
- 

Step 5: Check the result.

#Receiver sends an IGMPv2 member report packet to join the multicast group 225.1.1.1.

#Source sends a multicast service packet of the multicast group 225.1.1.1.

#View the multicast membership table on Device 2.

```
Device2#show ip igmp groups
IGMP Connected Group Membership
Total 1 groups
Group Address  Interface      Uptime  Expires  Last Reporter  V1 Expires  V2 Expires
225.1.1.1     vlan4          00:06:01 00:04:06 2.0.0.2        stopped
```

#View the PIM-DM multicast routing table of Device 2.

```
Device2#show ip pim dense-mode mroute
PIM-DM Multicast Routing Table
Total 1 mroute entries
(192.168.1.1, 225.1.1.1)
Expire in: 00:02:35
RPF Neighbor: 1.0.0.1, Nexthop: 1.0.0.1, vlan3
Upstream IF: vlan3
Upstream State: Forwarding
Assert State: Loser
Downstream IF List:
vlan4, in 'olist':
Downstream State: NoInfo
```

Assert State: NoInfo

#Receiver can only receive the multicast service packet of the multicast group 225.1.1.1 sent by Source.

---

 **Note**

- Information of Device 1 is viewed the same way as that of Device 2.
-

# 70 PIM-SM

---

## 70.1 Overview

PIM-SM (Protocol Independent Multicast-Spare Mode) is mainly applicable to the cases where the distribution of group members is relatively spare and the range is wide, or the network bandwidth resources are limited.

PIM-SM is independent of the specific unicast routing protocol. The device actively sends a join packet to request the establishment of a multicast distribution tree, and sets RP (Rendezvous Point) and BSR (Bootstrap Router) to advertise the multicast information to all the PIM-SM routers. When the receiver joins one multicast group, the receiving DR (Designated Router) sends a PIM join packet to RP to construct the shared tree rooted at RP—RPT. The source DR registers the multicast source with RP and constructs the active tree rooted at the multicast source. Multicast service packets are transmitted down the active tree and the shared tree to the receiver. The receiving DR will send the PIM join packet to the multicast source, and finally switch from RPT to the source-based shortest path tree SPT to reduce network latency.

PIM-SSM is Protocol Independent Multicast-Source Specific Multicast. PIM-SSM is a subset of the PIM-SM protocol and must run on the basis of PIM-SM. The PIM-SSM protocol stipulates that IPv4 addresses 232.0.0.0-232.255.255.255 are reserved for SSM. PIM-SSM needs to be used in conjunction with IGMPv3, because IGMPv3 can send IGMP membership reports for specified sources and groups.

## 70.2 PIM-SM Function Configuration

Table 70-1 PIM-SM Function Configuration List

Configuration Task	
Configure basic functions of PIM-SM	Enable PIM-SM protocol
	Configure C-RP

Configuration Task	
Configure PIM-SM aggregation router	Configure static RP
Configure PIM-SM bootstrap router	Configure C-BSR
	Configure BSR Border
Configure PIM-SM multicast source registration	Configure RP reachability check
	Configure sending rate of register packets
	Configure sending rate of register-stop packets
	Configure source address of register packets
	Configure register packet filtering
Configure PIM-SM neighbor parameters	Configure sending period of HELLO packets
	Configure keepalive time of neighbors
	Configure neighbor filtering
	Configure DR priority
Configure PIM-SM SPT switching	Configure SPT switching conditions
Configure PIM-SSM	Configure PIM-SSM
Configure PIM-SDM	Enable PIM-SDM

## Caution

- The L3 Ethernet interface does not support the PIM-SM function.

## 70.2.1 Configure basic functions of PIM-SM

### Configuration Condition

Before configuring PIM-SM, do the following:

- Configure the network layer address of the interface so that all neighbor nodes are reachable at the network layer;
- Configure any unicast routing protocol to achieve reachable routes within the domain.

### Enable PIM-SM protocol

Table 70–2 Enabling PIM-SM Protocol

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable IP multicast forwarding	<b>ip multicast-routing</b>	Mandatory By default, IP multicast forwarding is not enabled
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Enable PIM-SM protocol	<b>ip pim sparse-mode</b>	Either-or
	<b>ip pim sparse-mode passive</b>	By default, the interface is in PIM-SM shut-down state

---

 **Note**

- After enabling the PIM-SM protocol, the IGMP protocol is automatically enabled.
  - All PIM-SM-related configurations can only take effect after PIM-SM is enabled.
- 

## 70.2.2 Configure PIM-SM aggregation router

### Configuration Condition

Before configuring RP, do the following:

- Configure the network layer address of the interface so that all neighbor nodes are reachable at the network layer;
- Configure any unicast routing protocol to achieve reachable routes within the domain;
- Enable the PIM-SM protocol.

### Configure C-RP

RP results from C-RP election. After BSR election, all C-RPs (Candidate-Rendezvous Point, candidate aggregation routers) regularly unicast C-RP packets to BSR. BSR integrates the C-RP information and conveys the information to all the devices within the SM domain via bootstrap packets.

Table 70–3 Configuring C-RP

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure C-RP	<b>ip pim rp-candidate</b> <i>interface-name</i> [ [ <i>priority-value</i> [ <i>interval-value</i> [ <b>group-list</b> { <i>access-list-number</i>   <i>access-list-name</i> } ] ] ]   [ <b>group-list</b> { <i>access-list-number</i>	Mandatory  By default, there are no C-RPs

Step	Command	Description
	<code>access-list-name } ] ] [ vrf vrf-name ]</code>	

## Note

- RP election is performed based on the following rules:
  - 1, the longest mask matching is performed on the range of groups served by C-RP services;
  - 2, compare the C-RP priorities if there are multiple C-RPs in the longest mask matching, the smaller the value, the higher the priority, and those with the higher priority win;
  - 3, calculate the HASH value for the C-RP addresses and groups if there is more than one C-RP with the highest priority, and the C-RP with the largest HASH value wins;
  - 4, if there is more than one RP with the largest HASH value, the C-RP with the largest IP address wins.

### Configure static RP

For simple PIM-SM networks, the static RP is recommended. The use of the static RP eliminates the need for BSR configuration and eliminates frequent interaction between RPs and BSRs, thereby saving network bandwidth.

Table 70–4 Configuring Static RP

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure static RP	<b>ip pim rp-addressess</b> <i>ip-address</i> [ <i>access-list-name</i>   <i>access-list-number</i> ] [ <b>override</b> ] [ <i>vrf vrf-name</i> ]	Mandatory By default, there are no static RPs

---

 **Note**

- All devices in the same PIM-SM domain must be configured with the same static RP to work normally.
- 

### 70.2.3 Configure PIM-SM bootstrap router

#### Configuration Condition

Before configuring BSR, do the following:

- Configure the network layer address of the interface so that all neighbor nodes are reachable at the network layer;
- Configure any unicast routing protocol to achieve reachable routes within the domain;
- Enable the PIM-SM protocol.

#### Configure C-BSR

In one PIM-SM domain, there must be unique BSR. Multiple C-BSRs (Candidate-Bootstrap Routers) result in the only recognized BSR via bootstrap packet election.

Table 70-5 Configuring C-BSR

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure C-BSR	<b>ip pim bsr-candidate</b> <i>interface_name</i> [ <i>hash-mask-length</i> [ <i>priority-value</i> ] ] [ <b>vrf</b> <i>vrf-name</i> ]	Mandatory  By default, there are no C-BSRs

---

 **Note**

- 
- BSR election is performed based on the following rules:
    - 1, compare the priorities, the larger the value, the higher the priority, and those with the higher priority win;
    - 2, in the case of the same priority, those with the larger IP address win.
- 

### Configure BSR Border

BSR is responsible for collecting C-RP information and conveying this information to all devices within the PIM-SM domain via bootstrap packets. The range of BSR is also the range of the multicast domain. Bootstrap packets cannot pass through the interfaces configured with BSR border. The devices outside the multicast domain cannot forward multicast service packets within the multicast domain. In this way, the multicast domain is divided.

Table 70-6 Configure BSR Border

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure BSR Border	<b>ip pim bsr-border</b>	Mandatory By default, there are no multicast borders

## 70.2.4 Configure PIM-SM multicast source registration

### Configuration Condition

Before configuring multicast source registration, do the following:

- Configure the network layer address of the interface so that all neighbor

nodes are reachable at the network layer;

- Configure any unicast routing protocol to achieve reachable routes within the domain;
- Enable the PIM-SM protocol.

### Configure RP reachability check

Before the source DR sends the register packet to RP, you may run the reachability check on RP. If RP routing is found to be unreachable, skip registering with RP, thereby reducing the overhead of this DR.

Table 70-7 Configuring RP Reachability Check

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure RP reachability check	<b>ip pim register-rp-reachability</b> [ <i>vrf vrf-name</i> ]	Mandatory  By default, RP reachability is not checked before the registration process of PIM

---

### Note

- To reduce the overhead of the source DR, it is recommended to configure this command on all source DRs of PIM-SM.
- 

### Configure sending rate of register packets

When the source DR receives a multicast data packet, it encapsulates the multicast data packet into a register message and sends it to RP for source registration until the registration is completed.

When the source DR has not completed the registration of the multicast source and the multicast traffic is large, a large number of register packets will be generated, which will

increase the burden on the RP device, and even may cause RP not to work normally. Because it is not necessary for the source DR to send all the register packets of the same flow to RP, configuring the sending rate of the register packets at the source DR can meet the purpose of source registration and reduce the burden on RP.

Table 70-8 Configuring Sending Rate of Register Packets

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure sending rate of register packets	<b>ip pim register-rate-limit <i>rate-limit-value</i> [ <i>vrf vrf-name</i> ]</b>	Mandatory By default, the sending rate of register packets is not limited

---

 **Note**

- To reduce the burden on RP, it is recommended to configure the source registration sending rate on all source DRs.
- 

### Configure sending rate of register-stop packets

After RP receives a register packet from the source DR, it will send a register-stop packet to the source DR to complete the registration process. When RP receives many register packets, it is necessary to reply to all the register packets(that is, to send register-stop packets). In actual situations, there are many duplicate packets in these register-stop packets. The sending rate of the register-stop packets on RP can be limited to achieve the purpose of reducing the overhead on RP.

Table 70-9 Configuring Sending Rate of Register-stop Packets

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure sending rate of register-stop packets	<b>ip pim register-stop-rate-limit</b> <i>rate-limit-value</i> [ <b>vrf</b> <i>vrf-name</i> ]	Mandatory By default, the sending rate of register-stop packets is not limited

### Note

- To improve the robustness of the entire PIM-SM network, it is recommended to limit the rate of source register-stop packets in all RPs.

### Configure source address of register packets

When the source DR performs source registration, the source address of the register packet uses the register interface IP address automatically generated by the system. This command can specify the source address of the register packet as the IP address of one interface on this device to satisfy some special needs of the network.

Table 70-10 Configuring Source Address of Register Packets

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure source address of register packets	<b>ip pim register-source</b> <b>interface</b> <i>interface-name</i> [ <b>vrf</b> <i>vrf-name</i> ]	Mandatory By default, the IP address of the register interface automatically generated by the

Step	Command	Description
		system is used as the source address of the register packet

### Configure register packet filtering

To prevent source registration attacks, ACL can be used on RP to filter the multicast source for the register packets. Only the multicast sources allowed by the ACL can successfully register with RP.

Table 70-11 Configuring Register Packet Filtering

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure register packet filtering	<b>ip pim accept-register list</b> { <i>access-list-number</i>   <i>aces-list-name</i> } [ <i>vrf vrf-name</i> ]	Mandatory By default, register packets are not filtered

## 70.2.5 Configure PIM-SM neighbor parameters

### Configuration Condition

Before configuring PIM-SM neighbor parameters, do the following:

- Configure the network layer address of the interface so that all neighbor nodes are reachable at the network layer;
- Configure any unicast routing protocol to achieve reachable routes within the domain;
- Enable the PIM-SM protocol.

### Configure sending period of HELLO packets

The interface with the PIM protocol enabled will periodically send the Hello packet to establish and maintain PIM neighbors.

Table 70-12 Configuring Sending Period of Hello packets

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure sending period of HELLO packets	<b>ip pim hello-interval</b> <i>interval-value</i>	Optional By default, the interval of sending the Hello packet is 30 seconds

### Configure keepalive time of neighbors

When the Hello packet from one neighbor is received on the interface, the holdtime carried in the Hello packet will be recorded as the keepalive time of this neighbor. If no Hello packet of the neighbor is received within the keepalive period, this neighbor is considered invalid.

Table 70-13 Configuring PIM-DM Neighbor Keepalive Time

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure keepalive time of neighbors	<b>ip pim hello-holdtime</b> <i>holdtime-value</i>	Optional

Step	Command	Description
		By default, the keepalive time of the PIM-DM neighbors is 105 seconds

### Configure neighbor filtering

If there are many PIM neighbors in one subnet, you can use the neighbor filtering function to selectively establish the neighbor, thereby saving device resources.

Table 70-14 Configuring Neighbor Filtering

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure neighbor filtering	<b>ip pim neighbor-filter</b> { <i>access-list-number</i>   <i>access-list-name</i> }	Mandatory By default, the neighbor filtering function is not enabled

### Configure DR priority

DR plays a very important role in the PIM-SM network, so it is very important to select the appropriate DR. You can select the appropriate device as DR by configuring the DR priority.

Only one DR is allowed in one PIM-SM subnet, which can be divided into source DR and receiving DR according to functionality.

The main function of the source DR is to register the source with RP.

The main function of the receiving DR is to join RP and establish a switch between RPT and SPT.

Table 70-15 Configuring DR Priority

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure DR priority	<b>ip pim dr-priority</b> <i>priority-value</i>	Optional By default, the DR priority is 1

### Note

- DR election is performed based on the following rules:
  - 1、 compare the priorities, the larger the value, the higher the priority, and those with the higher priority win;
  - 2, in the case of the same priority, those with the larger IP address win.

## 70.2.6 Configure PIM-SM SPT switching

### Configuration Condition

Before configuring SPT, do the following:

- Configure the network layer address of the interface so that all neighbor nodes are reachable at the network layer;
- Configure any unicast routing protocol to achieve reachable routes within the domain;
- Enable the PIM-SM protocol.

### Configure SPT switching conditions

The receiving DR does not know the address of the multicast source, so it can only join RP to form RPT. The source DR will register the source with RP to form the active tree between the source DR and RP. At the beginning, the direction of the multicast stream is from the multicast source to RP, and then from RP to the receiver. When the receiving DR receives the first multicast data packet, it joins the multicast source to form SPT and prunes RPT. This process is called SPT switching.

This command functions to configure SPT switching conditions at the receiving DR.

Table 70-16 Configuring SPT Switching Conditions

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure SPT switching conditions	<b>ip pim spt-threshold infinity</b> [ <b>group-list</b> { <i>access-list-number</i>   <i>access-list-name</i> } ] [ <b>vrf vrf-name</b> ]	Mandatory  By default, all multicast groups undergo SPT switching

---

### Caution

- You must not configure SPT on RP to never switch; otherwise, this will cause multicast forwarding to fail.
- 

## 70.2.7 Configure PIM-SSM

PIM-SSM is a subset of PIM-SM. In PIM-SSM, there is no need for RP, BSR, or RPT, and there is no SPT switching. Instead, the receiving DR directly joins the multicast source and establishes the shortest path tree (SPT) rooted on the source.

### Configuration Condition

Before configuring PIM-SSM, do the following:

- Configure the network layer address of the interface so that all neighbor

nodes are reachable at the network layer;

- Configure any unicast routing protocol to achieve reachable routes within the domain;
- Enable the PIM-SM protocol on all interfaces on which multicast routing forwarding is to be carried.

### Configure PIM-SSM

Table 70-17 Configuring PIM-SSM

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure PIM-SSM	<b>ip pim ssm { default   range { access-list-number   access-list-name } } [ vrf vrf-name ]</b>	Mandatory By default, the SSM function is not enabled

---

### Caution

- When using PIM-SSM, ensure that IGMPv3 is enabled on the receiving DR;
  - In the case that the receiver cannot upgrade to IGMPv3, you can use the IGMP SSM Mapping function with PIM-SSM;
  - Ensure that the SSM multicast group address ranges configured on all devices in the domain are consistent, otherwise PIM-SSM may be abnormal.
- 

## 70.2.8 Configure Adaptive Basic Functions of PIM

### Configuration Condition

Before configuring PIM-SDM, do the following:

- Configure the network layer address of the interface so that all neighbor nodes are reachable at the network layer;
- Configure any unicast routing protocol to achieve reachable routes within the domain;

## Configure Adaptive Basic Functions of PIM

Table 70–18 Configuring PIM-SDM

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable IP multicast forwarding	<b>ip multicast-routing [ vrf vrf-name ]</b>	Mandatory By default, IP multicast forwarding is not enabled
Enter the interface configuration mode	<b>interface interface-name</b>	-
Configure adaptive function of PIM	<b>ip pim sparse-dense-mode</b>	Either-or By default, the adaptive function of PIM are shut down
	<b>ip pim sparse-dense-mode passive</b>	

---

### Note

After the adaptive function of PIM is enabled on the interface, the PIM-SM, PIM-DM, and IGMP protocols will be automatically enabled.

---

## 70.2.9 Configure PIM-SM Control Policy

### Configure Interface Attention for DR State Change

For non-DR, enable L2 multicast forwarding and stop L3 multicast forwarding. DR is not affected.

Table 70–19 Configuring DR Priority

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure DR priority	<b>ip pim drchg-attention</b>	L3 multicast forwarding is on by default

### Configure Interface Suppression for PIM JOIN Packets

Configuring interface requires suppression of PIM JOIN packets.

Table 70-20 Configuring Interface Suppression for PIM JOIN Packets

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure Interface Suppression for PIM JOIN Packets	<b>ip pim join-suppression</b>	By default, interface PIM JOIN packets are not suppressed

### 70.2.10 Configure PIM-SM Support (\*, \*, rp)

#### Configuration Condition

Before configuring PIM-SM Support (\*, \*, rp), do the following:

- Configure the network layer address of the interface so that all neighbor nodes are reachable at the network layer.
- Configure any unicast routing protocol to achieve reachable routes within the domain.
- Enable the PIM-SM protocol.

### Enable Support (\*, \*, rp)

Table 70–21 Enabling PIM-SM Protocol Support (\*, \*, rp)

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable PIM-SM support (*, *, rp)	<b>ip pim mbr [vrf vrf-name]</b>	Mandatory By default, support (*, *, rp) is not enabled

## 70.2.11 Configure PIM-SM BFD

### Configuration Condition

Before configuring PIM-SM BFD, do the following:

- Configure the network layer address of the interface so that all neighbor nodes are reachable at the network layer;
- Configure any unicast routing protocol to achieve reachable routes within the domain.

### Configure PIM-SM BFD

Table 70–22 Configuring PIM-SM BFD

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Enable PIM-SM BFD	<b>ip pim bfd</b>	By default, the PIM-SM BFD function is not enabled

## 70.2.12 PIM-SM Monitoring and Maintaining

Table 70-23 PIM-SM Monitoring and Maintaining

Command	Description
<b>clear ip pim bsr rp-set</b> [ <i>vrf vrf-name</i> ]	Clear RP set information of PIM-SM
<b>clear ip pim mroute</b> [ <i>group-address</i> [ <i>source-address</i> ] ] [ <i>vrf vrf-name</i> ]	Clear multicast routing information of PIM-SM
<b>clear ip pim statistics</b> [ <i>interface interface-name</i>   <i>vrf vrf-name</i> ]	Clear statistics of PIM-SM protocol packets
<b>show ip pim bsr-router</b> [ <i>vrf vrf-name</i> ]	Show PIM-SM bootstrap router information
<b>show ip pim interface</b> [ [ <i>interface-name</i> ] <b>detail</b> ] [ <i>vrf vrf-name</i> ]	Show PIM-SM interface information
<b>show ip pim local-members</b> [ <i>interface-name</i>   <i>vrf vrf-name</i> ]	Show PIM-SM local member information
<b>show ip pim mroute</b> [ <i>ssm</i>   <i>group group-ip-address</i> [ <i>source source-</i>	Show PIM-SM multicast routing table information

Command	Description
<i>ip-address</i> ]   <b>source</b> <i>source-ip-address</i> ] [ <b>vrf</b> <i>vrf-name</i> ]	
<b>show ip pim neighbor</b> [ <b>detail</b> ] [ <b>vrf</b> <i>vrf-name</i> ]	Show PIM-SM neighbor information
<b>show ip pim nexthop</b> [ <i>ip-address</i> ] [ <b>vrf</b> <i>vrf-name</i> ]	Show PIM-SM next hop router information
<b>show ip pim rp mapping</b> [ <b>vrf</b> <i>vrf-name</i> ]	Show PIM-SM RP information
<b>show ip pim rp-hash</b> <i>group-address</i> [ <b>vrf</b> <i>vrf-name</i> ]	Show RP information for multicast group mapping
<b>show ip pim statistics</b> [ <b>vrf</b> <i>vrf-name</i> ]	Show statistics of PIM-SM protocol packets

## 70.3 PIM-SM Typical Configuration Example

### 70.3.1 Configure basic functions of PIM-SM

#### Network Requirements

- The PIM-SM protocol runs on the entire network.
- Receiver 1 and Receiver 2 are two receivers of the Device 3 stub network.
- Device 1 and Device 2 are C-BSR and C-RP.
- IGMPv2 runs between Device 3 and the stub network.

#### Network Topology

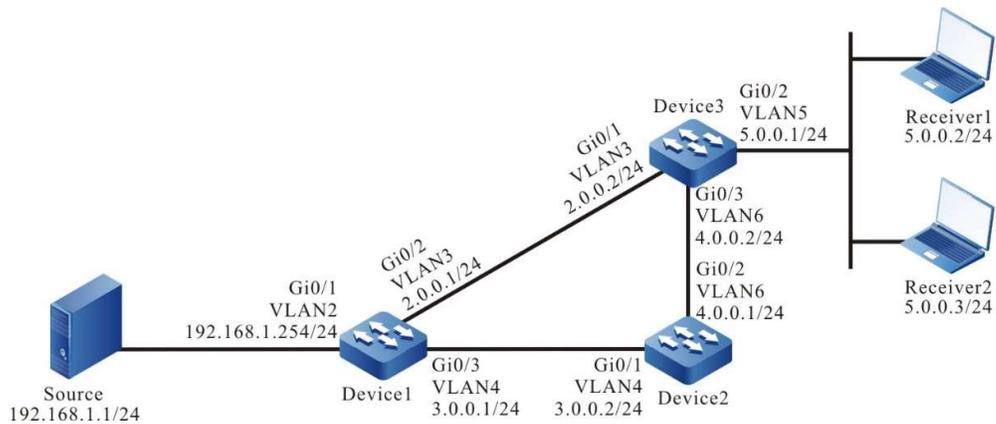


Figure 70-1 Network Topology for Configuring Basic Functions of PIM-SM

### Configuration Steps

- Step 1: Configure IP addresses for the ports. (Omitted)
- Step 2: Enable the unicast routing protocol OSPF, so that all devices in the network can communicate with each other.

#### #Configure Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 3.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 192.168.1.0 0.0.0.255 area 0
Device1(config-ospf)#exit
```

#### #Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 3.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#network 4.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#exit
```

#### #Configure Device3.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 4.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#exit
```

### #Check the routing table of Device3.

```
Device3#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C 2.0.0.0/24 is directly connected, 14:48:47, vlan3
O 3.0.0.0/24 [110/2] via 2.0.0.1, 14:31:14, vlan3
   [110/2] via 4.0.0.1, 14:31:04, vlan6
C 4.0.0.0/24 is directly connected, 15:36:57, vlan6
C 5.0.0.0/24 is directly connected, 14:09:18, vlan5
O 192.168.1.0/24 [110/2] via 2.0.0.1, 00:30:55, vlan3
```

---

### Note

- Device1 and Device2 are checked in the same way as Device3, the process of which is omitted.
- 

Step 3: Enable multicast forwarding globally, and enable the multicast protocol PIM-SM on the interfaces.

### #Configure Device1.

Enable multicast forwarding globally, and enable the multicast protocol PIM-SM on related interfaces.

```
Device1(config)#ip multicast-routing
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ip pim sparse-mode
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan3
Device1(config-if-vlan3)#ip pim sparse-mode
Device1(config-if-vlan3)#exit
Device1(config)#interface vlan4
Device1(config-if-vlan4)#ip pim sparse-mode
Device1(config-if-vlan4)#exit
```

### #Configure Device2.

Enable multicast forwarding globally, and enable the multicast protocol PIM-SM on related interfaces.

```
Device2(config)#ip multicast-routing
Device2(config)#interface vlan4
Device2(config-if-vlan4)#ip pim sparse-mode
Device2(config-if-vlan4)#exit
Device2(config)#interface vlan6
Device2(config-if-vlan6)#ip pim sparse-mode
Device2(config-if-vlan6)#exit
```

### #Configure Device3.

Enable multicast forwarding globally, and enable the multicast protocol PIM-SM on related interfaces.

```
Device3(config)#ip multicast-routing
Device3(config)#interface vlan3
Device3(config-if-vlan3)#ip pim sparse-mode
Device3(config-if-vlan3)#exit
Device3(config)#interface vlan5
Device3(config-if-vlan5)#ip pim sparse-mode
Device3(config-if-vlan5)#exit
Device3(config)#interface vlan6
Device3(config-if-vlan6)#ip pim sparse-mode
Device3(config-if-vlan6)#exit
```

#View, for Device 3, interface information with PIM-SM protocol enabled and PIM-SM neighbor information.

```
Device3#show ip pim interface
PIM Interface Table:
PIM VRF Name: Default
Total 3 Interface entries
Total 0 External Interface entry
Total 0 Sparse-Dense Mode Interface entry
```

Address	Interface	VIF Index	Ver/ Mode	VIF Flag	Nbr Count	DR Pri	DR	BSR	CISCO	Neighbor
								Border	Neighbor	Filter
2.0.0.2	vlan3	0	v2/S	UP	1 1	2.0.0.2	2.0.0.2	FALSE	FALSE	FALSE
5.0.0.1	vlan5	2	v2/S	UP	0 1	5.0.0.1	5.0.0.1	FALSE	FALSE	FALSE

```
4.0.0.2    vlan6          3    v2/S  UP  1    1    4.0.0.2    FALSE FALSE
```

```
Device3#show ip pim neighbor
```

```
PIM Neighbor Table:
```

```
PIM VRF Name: Default
```

```
Total 2 Neighbor entries
```

Neighbor Address	Interface	Uptime/Expires	Ver	DR
2.0.0.1	vlan3	01:12:00/00:01:39	v2	1 /
4.0.0.1	vlan6	01:13:19/00:01:35	v2	1 /

---

## Note

- Device1 and Device2 are checked in the same way as Device3, the process of which is omitted.
- 

#View the IGMP information of the interface vlan 5 of Device 3.

```
Device3#show ip igmp interface vlan5
```

```
Interface vlan5 (Index 50332250)
```

```
IGMP Active, Querier (5.0.0.1)
```

```
Default version 2
```

```
IP router alert option in IGMP V2 msgs: EXCLUDE
```

```
Internet address is 5.0.0.1
```

```
IGMP query interval is 125 seconds
```

```
IGMP querier timeout is 255 seconds
```

```
IGMP max query response time is 10 seconds
```

```
Last member query response interval is 1 seconds
```

```
Last member query count is 2
```

```
Group Membership interval is 260 seconds
```

```
IGMP robustness variable is 2
```

---

## Caution

- After the multicast protocol is configured on the interface, the IGMP function is automatically enabled, and IGMPv2 is run by default. By means of the
-

---

command **ip igmp version** you can configure the version of IGMP that runs on the interface.

---

Step 4: Configure the interface vlan 3 of Device 1 as C-BSR and C-RP, and configure the interface vlan 4 of Device 2 as C-BSR and C-RP.

#### #Configure Device1.

Configure the interface vlan 3 of Device 1 as C-BSR and C-RP. The priority of C-BSR is 200, and the range of multicast groups served by C-RP is 230.0.0.0/8.

```
Device1(config)#ip pim bsr-candidate vlan 3 10 200
Device1(config)#ip access-list standard 1
Device1(config-std-nacl)#permit 230.0.0.0 0.255.255.255
Device1(config-std-nacl)#commit
Device1(config-std-nacl)#exit
Device1(config)#ip pim rp-candidate vlan 3 group-list 1
```

#### #Configure Device2.

Configure vlan 4 of Device 2 as C-BSR and C-RP. The priority of C-BSR is 0, and the range of multicast groups served by C-RP of Device2 is 224.0.0.0/4.

```
Device2(config)#ip pim bsr-candidate vlan4
Device2(config)#ip pim rp-candidate vlan4
```

#### #View the BSR and RP information of Device 3

```
Device3#show ip pim bsr-router
PIMv2 Bootstrap information
PIM VRF Name: Default
  BSR address: 2.0.0.1
  BSR Priority: 200
Hash mask length: 10
Up time: 01:03:30
Expiry time: 00:01:46
Role: Non-candidate BSR
State: Accept Preferred
```

```
Device3#show ip pim rp mapping
PIM Group-to-RP Mappings Table:
```

PIM VRF Name: Default

Total 2 RP set entries

Total 2 RP entries

Group(s): 224.0.0.0/4

RP count: 1

RP: 3.0.0.2

Info source: 2.0.0.1, via bootstrap, priority 192

Up time: 01:03:29

Expiry time: 00:02:02

Group(s): 230.0.0.0/8

RP count: 1

RP: 2.0.0.1

Info source: 2.0.0.1, via bootstrap, priority 192

Up time: 01:15:50

Expiry time: 00:02:02

---

## Caution

- Device 1 and Device 2 are viewed the same way as Device 3, and the viewing process is omitted;
  - When multiple C-BSRs are configured in one multicast domain, BSR will be elected according to the priority first, and C-BSR with the highest priority will be elected as BSR. When the priorities of the C-BSRs are the same, the C-BSR with the largest ip address is elected as BSR;
  - When multiple C-RPs are configured in one multicast domain and the ranges of multicast groups served are the same, RP corresponding to the multicast group G will be calculated according to the hash algorithm;
  - You can also use the command **ip pim rp-address** in the multicast domain to configure RP, but the static RP addresses configured on all devices in the entire multicast domain must be consistent.
- 

Step 5: Check the result.

#Receiver 1 and Receiver 2 send IGMPv2 membership reports to join the multicast groups 225.1.1.1 and 230.1.1.1, respectively.

#Source sends the multicast service packets of the multicast groups 225.1.1.1 and 230.1.1.1.

#View the multicast membership table on Device 3.

```
Device3#show ip igmp groups
IGMP Connected Group Membership
Total 2 groups
Group Address  Interface      Uptime Expires Last Reporter  V1 Expires V2 Expires
225.1.1.1     vlan5          00:56:48 00:02:39 5.0.0.2        stopped
230.1.1.1     vlan5          00:56:48 00:02:46 5.0.0.3        stopped
```

#View the RPs corresponding to the multicast groups 225.1.1.1 and 230.1.1.1 on Device 3.

```
Device3#show ip pim rp-hash 225.1.1.1
PIM VRF Name: Default
RP: 3.0.0.2
Info source: 2.0.0.1, via bootstrap
```

```
Device3#show ip pim rp-hash 230.1.1.1
PIM VRF Name: Default
RP: 2.0.0.1
Info source: 2.0.0.1, via bootstrap
```

#View the multicast routing table of Device 3.

```
Device3#show ip pim mroute
IP Multicast Routing Table:
PIM VRF Name: Default
Total 0 (*,*,RP) entry
Total 2 (*,G) entries
Total 2 (S,G) entries
Total 2 (S,G,rpt) entries
Total 0 FCR entry
Up timer/Expiry timer
(*,225.1.1.1)
Up time: 00:36:21
RP: 3.0.0.2
RPF nbr: 4.0.0.1
RPF idx: vlan6
Flags:
JOIN DESIRED
Upstream State: JOINED
```

Local interface list:  
vlan5  
Joined interface list:  
Asserted interface list:

(192.168.1.1, 225.1.1.1)

Up time: 00:36:02

KAT time: 00:03:11

RPF nbr: 4.0.0.1

RPF idx: vlan6

SPT bit: TRUE

Flags:

JOIN DESIRED

Upstream State: JOINED

Local interface list:

Joined interface list:

Asserted interface list:

Outgoing interface list:

vlan5

Packet count 2517423

(192.168.1.1, 225.1.1.1, rpt)

Up time: 00:36:02

RP: 3.0.0.2

Flags:

RPT JOIN DESIRED

PRUNE DESIRED

RPF SGRPT XG EQUAL

Upstream State: PRUNED

Local interface list:

Pruned interface list:

Outgoing interface list:

vlan5

(\* , 230.1.1.1)

Up time: 00:36:21

RP: 2.0.0.1

RPF nbr: 2.0.0.1

RPF idx: vlan3  
Flags:  
JOIN DESIRED  
Upstream State: JOINED  
Local interface list:  
vlan5  
Joined interface list:  
Asserted interface list:

(192.168.1.1, 230.1.1.1)

Up time: 00:36:02  
KAT time: 00:03:11  
RPF nbr: 2.0.0.1  
RPF idx: vlan3  
SPT bit: TRUE

Flags:  
JOIN DESIRED  
Upstream State: JOINED  
Local interface list:  
Joined interface list:  
Asserted interface list:  
Outgoing interface list:  
vlan5  
Packet count 2517712

(192.168.1.1, 230.1.1.1, rpt)

Up time: 00:36:02  
RP: 2.0.0.1  
Flags:  
RPT JOIN DESIRED  
RPF SGRPT XG EQUAL  
Upstream State: NOT PRUNED  
Local interface list:  
Pruned interface list:  
Outgoing interface list:

#Receiver 1 can only receive the multicast service packet of the multicast group 225.1.1.1 sent by Source. Receiver2

can only receive the multicast service packet of the multicast group 230.1.1.1 sent by Source.

---

## Note

- Device1 and Device2 are checked in the same way as Device3, the process of which is omitted.
  - By default, SPT switching is enabled on the device.
- 

## 70.3.2 Configure PIM-SSM

### Network Requirements

- The PIM-SSM protocol runs on the entire network.
- Receiver is one receiver of the Device 3 stub network.
- IGMPv3 runs between Device 3 and the stub network.

### Network Topology

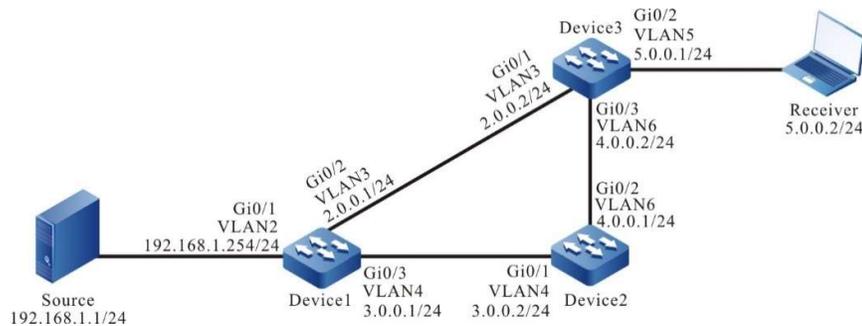


Figure 70-2 Network Topology for Configuring PIM-SSM

### Configuration Steps

- Step 1: Configure IP addresses for the ports. (Omitted)
- Step 2: Enable the unicast routing protocol OSPF, so that all devices in the network can communicate with each other.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 3.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 192.168.1.0 0.0.0.255 area 0
Device1(config-ospf)#exit
```

### #Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 3.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#network 4.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#exit
```

### #Configure Device3.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 4.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#exit
```

### #Check the routing table of Device3.

```
Device3#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C 2.0.0.0/24 is directly connected, 14:48:47, vlan3
O 3.0.0.0/24 [110/2] via 2.0.0.1, 14:31:14, vlan3
   [110/2] via 4.0.0.1, 14:31:04, vlan6
C 4.0.0.0/24 is directly connected, 15:36:57, vlan6
C 5.0.0.0/24 is directly connected, 14:09:18, vlan5
O 192.168.1.0/24 [110/2] via 2.0.0.1, 00:30:55, vlan3
```

---

## Note

- Device1 and Device2 are checked in the same way as Device3, the process of which is omitted.

Step 3: Enable multicast forwarding globally, and enable the multicast protocol PIM-SM on the interfaces.

#### #Configure Device1.

Enable multicast forwarding globally, and enable the multicast protocol PIM-SM on related interfaces.

```
Device1(config)#ip multicast-routing
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ip pim sparse-mode
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan3
Device1(config-if-vlan3)#ip pim sparse-mode
Device1(config-if-vlan3)#exit
Device1(config)#interface vlan4
Device1(config-if-vlan4)#ip pim sparse-mode
Device1(config-if-vlan4)#exit
```

#### #Configure Device2.

Enable multicast forwarding globally, and enable the multicast protocol PIM-SM on related interfaces.

```
Device2(config)#ip multicast-routing
Device2(config)#interface vlan4
Device2(config-if-vlan4)#ip pim sparse-mode
Device2(config-if-vlan4)#exit
Device2(config)#interface vlan6
Device2(config-if-vlan6)#ip pim sparse-mode
Device2(config-if-vlan6)#exit
```

#### #Configure Device3.

Enable multicast forwarding globally, and enable the multicast protocol PIM-SM on related interfaces.

```
Device3(config)#ip multicast-routing
Device3(config)#interface vlan3
Device3(config-if-vlan3)#ip pim sparse-mode
Device3(config-if-vlan3)#exit
Device3(config)#interface vlan5
```

```

Device3(config-if-vlan5)#ip pim sparse-mode
Device3(config-if-vlan5)#exit
Device3(config)#interface vlan6
Device3(config-if-vlan6)#ip pim sparse-mode
Device3(config-if-vlan6)#exit

```

#View, for Device 3, interface information with PIM-SM protocol enabled and PIM-SM neighbor information.

```

Device3#show ip pim interface
PIM Interface Table:
PIM VRF Name: Default
Total 3 Interface entries
Total 0 External Interface entry
Total 0 Sparse-Dense Mode Interface entry

```

Address	Interface	VIF Index	Ver/ Mode	VIF Flag	Nbr Count	DR Pri	DR	BSR	CISCO	Neighbor
								Border Neighbor Filter		
2.0.0.2	vlan3	3	v2/S	UP	1 1	2.0.0.2		FALSE	FALSE	
5.0.0.1	vlan5	0	v2/S	UP	0 1	5.0.0.1		FALSE	FALSE	
4.0.0.2	vlan6	2	v2/S	UP	1 1	4.0.0.2		FALSE	FALSE	

```

Device3#show ip pim neighbor
PIM Neighbor Table:
PIM VRF Name: Default
Total 2 Neighbor entries
Neighbor Interface Uptime/Expires Ver DR
Address Priority/Mode
2.0.0.1 vlan3 01:12:00/00:01:39 v2 1 /
4.0.0.1 vlan6 01:13:19/00:01:35 v2 1 /

```

---

## Note

- Device1 and Device2 are checked in the same way as Device3, the process of which is omitted.
-

Step 4: Configure PIM-SSM on all devices. The range of multicast groups served by SSM is 232.0.0.0/8. IGMPv3 is run on vlan 5 of Device 3.

#Configure Device1.

```
Device1(config)#ip pim ssm default
```

#Configure Device2.

```
Device2(config)#ip pim ssm default
```

#Configure Device3.

```
Device3(config)#ip pim ssm default
Device3(config)#interface vlan5
Device3(config-if-vlan5)#ip igmp version 3
Device3(config-if-vlan5)#exit
```

#View the IGMP information of the interface vlan 5 of Device 3.

```
Device3#show ip igmp interface vlan5
Interface vlan5 (Index 50332250)
IGMP Enabled, Active, Querier (5.0.0.1)
Configured for version 3
IP router alert option in IGMP V2 msgs: EXCLUDE
Internet address is 5.0.0.1
IGMP query interval is 125 seconds
IGMP querier timeout is 255 seconds
IGMP max query response time is 10 seconds
Last member query response interval is 1 seconds
Last member query count is 2
Group Membership interval is 260 seconds
IGMP robustness variable is 2
```

Step 5: Check the result.

#Receiver sends the IGMPv3 membership report of the specified source group to join the multicast group 232.1.1.1, and the specified multicast source is 192.168.1.1.

#Source sends the multicast service packet of the multicast group 232.1.1.1.

#View the multicast membership table of Device 3.

```
Device3#show ip igmp groups
IGMP Connected Group Membership
```

```
Total 1 groups
Group Address Interface Uptime Expires Last Reporter V1 Expires V2 Expires
232.1.1.1 vlan5 00:11:14 stopped 5.0.0.2 stopped stopped
```

```
Device3#show ip igmp groups detail
```

```
Interface: vlan5
Group: 232.1.1.1
Uptime: 00:11:20
Group mode: Include
Last reporter: 5.0.0.2
TIB-A Count: 1
TIB-B Count: 0
Group source list: (R - Remote, M - SSM Mapping)
Source Address Uptime v3 Exp M Exp Fwd Flags
192.168.1.1 00:11:20 00:03:28 stopped Yes R
```

### #View the multicast routing table of Device 3.

```
Device3#show ip pim mroute
```

```
IP Multicast Routing Table:
```

```
PIM VRF Name: Default
```

```
Total 0 (*,*,RP) entry
```

```
Total 0 (*,G) entry
```

```
Total 1 (S,G) entry
```

```
Total 0 (S,G,rpt) entry
```

```
Total 0 FCR entry
```

```
Up timer/Expiry timer
```

```
(192.168.1.1, 232.1.1.1)
```

```
Up time: 12:59:27
```

```
KAT time: 00:03:20
```

```
RPF nbr: 2.0.0.1
```

```
RPF idx: vlan3
```

```
SPT bit: TRUE
```

```
Flags:
```

```
JOIN DESIRED
```

```
Upstream State: JOINED
```

```
Local interface list:
```

```
vlan5
```

```
Joined interface list:
```

Asserted interface list:

Outgoing interface list:

vlan5

Packet count 109783214

#Receiver can receive the multicast service packet of the multicast group 232.1.1.1 sent by Source.

---

## Note

- Device 1 and Device 2 are viewed the same way as Device 3, and the viewing process is omitted.
  - The default multicast group range of PIM-SSM is 232.0.0.0/8. The range of multicast groups served by PIM-SSM can be modified with the command `ip pim ssm range`.
  - For the multicast group G that meets the SSM conditions, the multicast routing table will not generate entry (\*, G), but only entry (S, G).
- 

### 70.3.3 Configure PIM-SM Multicast Forwarding Control

#### Network Requirements

- The PIM-SM protocol runs on the entire network.
- Receiver is one receiver of the Device 3 stub network.
- Device 2 is C-BSR and C-RP.
- On Device 2 and Device 3, the multicast source is controlled so that Receiver can only receive the multicast service packet sent by Source 1.
- IGMPv2 runs between Device 3 and the stub network.

#### Network Topology

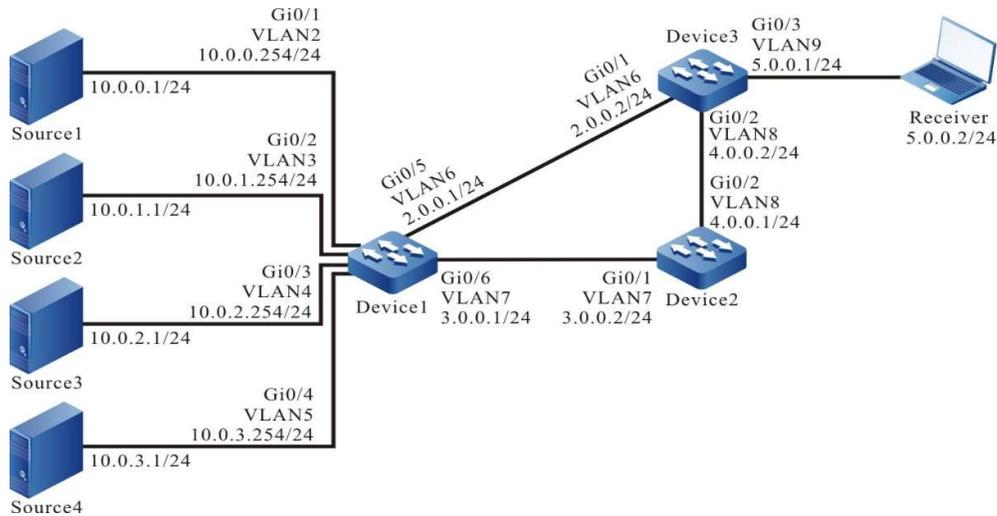


Figure 70-3 Network Topology for Configuring PIM-SM Multicast Forwarding Control

### Configuration Steps

Step 1: Configure IP addresses for the ports. (Omitted)

Step 2: Enable the unicast routing protocol OSPF, so that all devices in the network can communicate with each other.

#### #Configure Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 3.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 10.0.0.0 0.0.255.255 area 0
Device1(config-ospf)#exit
```

#### #Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 3.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#network 4.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#exit
```

#### #Configure Device3.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 4.0.0.0 0.0.0.255 area 0
```

```
Device3(config-ospf)#exit
```

### #Check the routing table of Device3.

```
Device3#show ip route
```

Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management

D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

```
C 2.0.0.0/24 is directly connected, 15:51:07, vlan6
```

```
O 3.0.0.0/24 [110/2] via 2.0.0.1, 15:33:34, vlan6  
[110/2] via 4.0.0.1, 15:33:24, vlan8
```

```
C 4.0.0.0/24 is directly connected, 16:39:17, vlan8
```

```
C 5.0.0.0/24 is directly connected, 15:11:38, vlan9
```

```
O 10.0.0.0/24 [110/2] via 2.0.0.1, 00:06:32, vlan6
```

```
O 10.0.1.0/24 [110/2] via 2.0.0.1, 00:06:32, vlan6
```

```
O 10.0.2.0/24 [110/2] via 2.0.0.1, 00:06:32, vlan6
```

```
O 10.0.3.0/24 [110/2] via 2.0.0.1, 00:06:32, vlan6
```

---

## Note

- Device 1 and Device 2 are viewed the same way as Device 3, and the viewing process is omitted.
- 

Step 3: Enable multicast forwarding globally, and enable the multicast protocol PIM-SM on the interfaces.

### #Configure Device1.

Enable multicast forwarding globally, and enable the multicast protocol PIM-SM on related interfaces.

```
Device1(config)#ip multicast-routing
```

```
Device1(config)#interface vlan2
```

```
Device1(config-if-vlan2)#ip pim sparse-mode
```

```
Device1(config-if-vlan2)#exit
```

```
Device1(config)#interface vlan3
```

```
Device1(config-if-vlan3)#ip pim sparse-mode
```

```
Device1(config-if-vlan3)#exit
Device1(config)#interface vlan4
Device1(config-if-vlan4)#ip pim sparse-mode
Device1(config-if-vlan4)#exit
Device1(config)#interface vlan5
Device1(config-if-vlan5)#ip pim sparse-mode
Device1(config-if-vlan5)#exit
Device1(config)#interface vlan6
Device1(config-if-vlan6)#ip pim sparse-mode
Device1(config-if-vlan6)#exit
Device1(config)#interface vlan7
Device1(config-if-vlan7)#ip pim sparse-mode
Device1(config-if-vlan7)#exit
```

### #Configure Device2.

Enable multicast forwarding globally, and enable the multicast protocol PIM-SM on related interfaces.

```
Device2(config)#ip multicast-routing
Device2(config)#interface vlan7
Device2(config-if-vlan7)#ip pim sparse-mode
Device2(config-if-vlan7)#exit
Device2(config)#interface vlan8
Device2(config-if-vlan8)#ip pim sparse-mode
Device2(config-if-vlan8)#exit
```

### #Configure Device3.

Enable multicast forwarding globally, and enable the multicast protocol PIM-SM on related interfaces.

```
Device3(config)#ip multicast-routing
Device3(config)#interface vlan6
Device3(config-if-vlan6)#ip pim sparse-mode
Device3(config-if-vlan6)#exit
Device3(config)#interface vlan8
Device3(config-if-vlan8)#ip pim sparse-mode
Device3(config-if-vlan8)#exit
Device3(config)#interface vlan9
Device3(config-if-vlan9)#ip pim sparse-mode
Device3(config-if-vlan9)#exit
```

#View, for Device 3, interface information with PIM-SM protocol enabled and PIM-SM neighbor information.

```
Device3#show ip pim interface
```

```
PIM Interface Table:
```

```
PIM VRF Name: Default
```

```
Total 3 Interface entries
```

```
Total 0 External Interface entry
```

```
Total 0 Sparse-Dense Mode Interface entry
```

Address	Interface	VIF Index	Ver/ Mode	VIF Flag	Nbr Count	DR Priority	DR	BSR	CISCO	Neighbor Border Neighbor Filter
2.0.0.2	vlan6	2	v2/S UP	1	1	2.0.0.2		FALSE	FALSE	
4.0.0.2	vlan8	0	v2/S UP	1	1	4.0.0.2		FALSE	FALSE	
5.0.0.1	vlan9	3	v2/S UP	0	1	5.0.0.1		FALSE	FALSE	

```
Device3#show ip pim neighbor
```

```
PIM Neighbor Table:
```

```
PIM VRF Name: Default
```

```
Total 2 Neighbor entries
```

Neighbor Address	Interface	Uptime/Expires	Ver	DR
2.0.0.1	vlan6	00:50:29/00:01:19	v2	1 /
4.0.0.1	vlan8	00:57:58/00:01:33	v2	1 /

---

## Note

- Device 1 and Device 2 are viewed the same way as Device 3, and the viewing process is omitted.
- 

Step 4: Configure vlan 7 of Device 2 as C-BSR and C-RP of the entire network. The range of multicast groups served by C-RP is 224.0.0.0/4.

#Configure Device2.

```
Device2(config)#ip pim bsr-candidate vlan7
```

```
Device2(config)#ip pim rp-candidate vlan7
```

### #View the BSR and RP information of Device 3.

```
Device3#show ip pim bsr-router
```

```
PIMv2 Bootstrap information
```

```
PIM VRF Name: Default
```

```
BSR address: 3.0.0.2
```

```
BSR Priority: 0
```

```
Hash mask length: 10
```

```
Up time: 00:10:37
```

```
Expiry time: 00:01:33
```

```
Role: Non-candidate BSR
```

```
State: Accept Preferred
```

```
Device3#show ip pim rp mapping
```

```
PIM Group-to-RP Mappings Table:
```

```
PIM VRF Name: Default
```

```
Total 1 RP set entry
```

```
Total 1 RP entry
```

```
Group(s): 224.0.0.0/4
```

```
RP count: 1
```

```
RP: 3.0.0.2
```

```
Info source: 3.0.0.2, via bootstrap, priority 192
```

```
Up time: 03:59:59
```

```
Expiry time: 00:01:49
```

---

### Note

- Device 1 and Device 2 are viewed the same way as Device 3, and the viewing process is omitted.
- 

Step 5: On Device 2 and Device 3, the multicast source is controlled so that Receiver can only receive the multicast service packet sent by Source 1.

#On Device 2, configure the access list of accepted registration messages to filter out the registration messages of Source 4.

```
Device2(config)#ip access-list standard 1
Device2(config-std-nacl)#deny 10.0.3.0 0.0.0.255
Device2(config-std-nacl)#permit any
Device2(config-std-nacl)#commit
Device2(config-std-nacl)#exit
Device2(config)#ip pim accept-register list 1
```

**#Configure incoming acl on interfaces vlan 6 and vlan 8 of Device 3 to filter out the multicast service packet of Source 3.**

```
Device3(config)#ip access-list extended 1001
Device3(config-ext-nacl)#deny ip 10.0.2.0 0.0.0.255 224.0.0.0 31.255.255.255
Device3(config-ext-nacl)#permit igmp any any
Device3(config-ext-nacl)#permit pim any any
Device3(config-ext-nacl)#permit ospf any any
Device3(config-ext-nacl)#permit ip any any
Device3(config-ext-nacl)commit
Device3(config-ext-nacl)#exit
Device3(config)#interface vlan6
Device3(config-if-vlan6)#ip access-group 1001 in
Device3(config-if-vlan6)#exit
Device3(config)#interface vlan8
Device3(config-if-vlan8)#ip access-group 1001 in
Device3(config-if-vlan8)#exit
```

**#Configure outgoing acl on interface vlan 9 of Device 3 to filter out the multicast service packet of Source 2.**

```
Device3(config)#ip access-list extended 1002
Device3(config-ext-nacl)#deny ip 10.0.1.0 0.0.0.255 224.0.0.0 31.255.255.255
Device3(config-ext-nacl)#permit igmp any any
Device3(config-ext-nacl)#permit pim any any
Device3(config-ext-nacl)#permit ip any any
Device3(config-ext-nacl)#commit
Device3(config-ext-nacl)#exit
Device3(config)#interface vlan9
Device3(config-if-vlan9)#ip access-group 1002 out
Device3(config-if-vlan9)#exit
```

**Step 6: Check the result.**

#Receiver sends an IGMPv2 membership report to join the multicast group 225.1.1.1.

Source 1, Source 2, Source 3, and Source 4 all send multicast service packets of the multicast group 225.1.1.1.

#View the multicast membership table of Device 2.

```
Device2#show ip igmp groups
IGMP Connected Group Membership
Total 1 groups
Group Address  Interface      Uptime  Expires  Last Reporter  V1 Expires  V2 Expires
225.1.1.1     vlan9          00:00:38 00:03:45 5.0.0.2        stopped
```

#View the multicast routing table of Device 3.

```
Device3#show ip pim mroute
IP Multicast Routing Table:
PIM VRF Name: Default
Total 0 (*,*,RP) entry
Total 1 (*,G) entry
Total 2 (S,G) entries
Total 2 (S,G,rpt) entries
Total 0 FCR entry
Up timer/Expiry timer
```

(\*, 225.1.1.1)

Up time: 00:07:55

RP: 3.0.0.2

RPF nbr: 4.0.0.1

RPF idx: vlan8

Flags:

JOIN DESIRED

Upstream State: JOINED

Local interface list:

vlan9

Joined interface list:

Asserted interface list:

(10.0.0.1, 225.1.1.1)

Up time: 00:07:49

KAT time: 00:03:17  
RPF nbr: 2.0.0.1  
RPF idx: vlan6  
SPT bit: TRUE  
Flags:  
JOIN DESIRED  
Upstream State: JOINED  
Local interface list:  
Joined interface list:  
Asserted interface list:  
Outgoing interface list:  
vlan9  
Packet count 268411

(10.0.0.1, 225.1.1.1, rpt)

Up time: 00:07:49  
RP: 3.0.0.2  
Flags:  
RPT JOIN DESIRED  
PRUNE DESIRED  
RPF SGRPT XG EQUAL  
Upstream State: PRUNED  
Local interface list:  
Pruned interface list:  
Outgoing interface list:  
vlan9

(10.0.1.1, 225.1.1.1)

Up time: 00:07:49  
KAT time: 00:03:17  
RPF nbr: 2.0.0.1  
RPF idx: vlan6  
SPT bit: TRUE  
Flags:  
JOIN DESIRED  
Upstream State: JOINED  
Local interface list:  
Joined interface list:

Asserted interface list:  
Outgoing interface list:  
vlan9  
Packet count 268237

(10.0.1.1, 225.1.1.1, rpt)

Up time: 00:07:49

RP: 3.0.0.2

Flags:

RPT JOIN DESIRED

PRUNE DESIRED

RPF SGRPT XG EQUAL

Upstream State: PRUNED

Local interface list:

Pruned interface list:

Outgoing interface list:

vlan9



- Device 1 and Device 2 are viewed the same way as Device 3, and the viewing process is omitted.
- 

#### #Check the matching status of acls on Device 2.

```
Device2#show ip access-list 1
ip access-list standard 1
10 deny 10.0.3.0 0.0.0.255 32 matches
20 permit any 2767 matches
```

#### #Check the matching status of acls on Device 3.

```
Device3#show ip access-list 1001
ip access-list extended 1001
10 deny ip 10.0.2.0 0.0.0.255 224.0.0.0 31.255.255.255 671545 matches
20 permit igmp any any 19 matches
30 permit pim any any 119 matches
40 permit ospf any any 252 matches
50 permit ip any any 1343339 matches
```

```
Device3#show ip access-list 1002
ip access-list extended 1002
10 deny ip 10.0.1.0 0.0.0.255 224.0.0.0 31.255.255.255 672358 matches
20 permit igmp any any 10 matches
30 permit pim any any 40 matches
40 permit ip any any 672532 matches
```

#Receive can only receive multicast service packets sent by Source 1.

---

## Caution

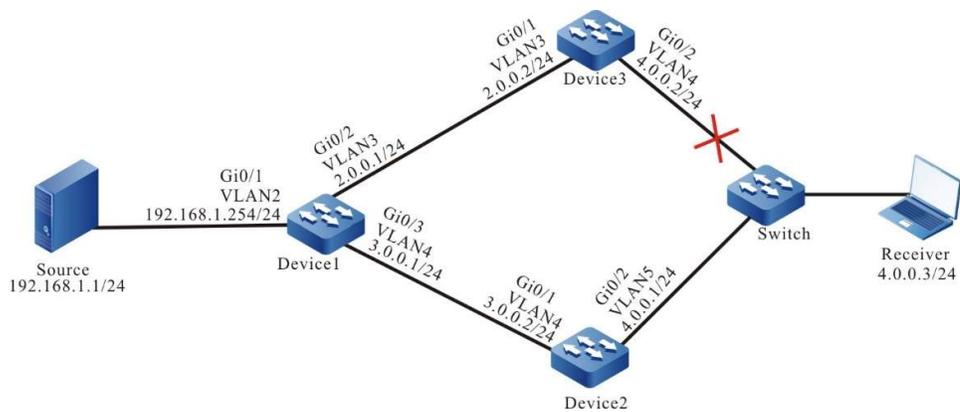
- When performing multicast source control, you are advised to configure multicast source control first and then demand the multicast source. By default, the receiving DR will switch SPTs after receiving the multicast service packet. If the multicast source is demanded before the multicast forwarding control is performed, the multicast forwarding control will not take effect. To prevent the multicast forwarding control from failing, you can configure SPT switching disallowed on the receiving DR.
- 

### 70.3.4 Configure DR Switching Convergence with PIM-SM and BFD Linkage

#### Network Requirements

- The PIM-SM protocol runs on the entire network.
- Device 1 is C-BSR and C-RP.
- Device 2 and Device 3 are located in the stub network where Receiver is located, and Device 3 acts as the receiver DR.
- PIM BFD is enabled on the line between Device 2 and Device 3. When the line between Device 3 and Receiver fails, Device 2 quickly switches to the receiver DR.

#### Network Topology



## 70-4 Network Topology for Configuring DR Switching with PIM-SM and BFD Linkage

### Configuration Steps

Step 1: Configure IP addresses for the interfaces (omitted).

Step 2: Enable the unicast routing protocol OSPF, so that all devices in the network can communicate with each other.

#### #Configure Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 3.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 192.168.1.0 0.0.0.255 area 0
Device1(config-ospf)#exit
```

#### #Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 3.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#network 4.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#exit
```

#### #Configure Device3.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 4.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#exit
```

### #Check the routing table of Device3.

```
Device3#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C 2.0.0.0/24 is directly connected, 14:48:47, vlan3
O 3.0.0.0/24 [110/2] via 2.0.0.1, 14:31:14, vlan3
   [110/2] via 4.0.0.1, 14:31:04, vlan4
C 4.0.0.0/24 is directly connected, 15:36:57, vlan4
O 192.168.1.0/24 [110/2] via 2.0.0.1, 00:30:55, vlan3
```



### Note

- Device1 and Device2 are checked in the same way as Device3, the process of which is omitted.
- 

Step 3: Enable multicast forwarding globally, and enable the multicast protocol PIM-SM on the interfaces.

### #Configure Device1.

Enable multicast forwarding globally and enable the multicast protocol PIM-SM on related interfaces.

```
Device1(config)#ip multicast-routing
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ip pim sparse-mode
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan 3
Device1(config-if-vlan3)#ip pim sparse-mode
Device1(config-if-vlan3)#exit
Device1(config)#interface vlan 4
Device1(config-if-vlan4)#ip pim sparse-mode
Device1(config-if-vlan4)#exit
```

### #Configure Device2.

Enable multicast forwarding globally and enable the multicast protocol PIM-SM on related interfaces.

```
Device2(config)#ip multicast-routing
Device2(config)#interface vlan 4
Device2(config-if-vlan4)#ip pim sparse-mode
Device2(config-if-vlan4)#exit
Device2(config)#interface vlan 5
Device2(config-if-vlan5)#ip pim sparse-mode
Device2(config-if-vlan5)#exit
```

### #Configure Device3.

Enable multicast forwarding globally and enable the multicast protocol PIM-SM on related interfaces.

```
Device3(config)#ip multicast-routing
Device3(config)#interface vlan 3
Device3(config-if-vlan3)#ip pim sparse-mode
Device3(config-if-vlan3)#exit
Device3(config)#interface vlan 4
Device3(config-if-vlan4)#ip pim sparse-mode
Device3(config-if-vlan4)#exit
```

#View, for Device 3, interface information with PIM-SM protocol enabled and PIM-SM neighbor information.

```
Device3#show ip pim interface
```

PIM Interface Table:

PIM VRF Name: Default

Total 2 Interface entries

Total 0 External Interface entry

Total 0 Sparse-Dense Mode Interface entry

Address	Interface	VIF Index	Ver/ Mode	VIF Flag	Nbr Count	DR	DR	BSR	CISCO	Neighbor
2.0.0.2	vlan3	2	v2/S	UP	1 1	2.0.0.2		FALSE	FALSE	
4.0.0.2	vlan4	0	v2/S	UP	1 1	4.0.0.2		FALSE	FALSE	

```
Device3#show ip pim neighbor
```

PIM Neighbor Table:

PIM VRF Name: Default

Total 2 Neighbor entries

NeighborInterface	Uptime/Expires	VerDR
Address	Priority/Mode	
4.0.0.1 vlan4	00:11:26/00:01:19	v2 1 /
2.0.0.1 vlan3	00:05:57/00:01:18	v2 1 /

#It is indicated that Device 3 is the receiver DR of the stub network where Receiver is located.

---

## Note

- Device1 and Device2 are checked in the same way as Device3, the process of which is omitted.
- 

Step 4: Configure C-BSR and C-RP.

#Configure Device1.

Configure vlan 2 of Device 1 as C-BSR and C-RP of the entire network. The range of multicast groups served by C-RP is 224.0.0.0/8.

```
Device1(config)#ip pim bsr-candidate vlan 2
Device1(config)#ip pim rp-candidate vlan 2
```

#View the BSR and RP information of Device 3.

```
Device3#show ip pim bsr-router
PIMv2 Bootstrap information
PIM VRF Name: Default
BSR address: 192.168.1.254
BSR Priority: 0
Hash mask length: 10
Up time: 00:00:17
Expiry time: 00:01:56
Role: Non-candidate BSR
State: Accept Preferred
```

```
Device3#show ip pim rp mapping
PIM Group-to-RP Mappings Table:
PIM VRF Name: Default
```

```
Total 1 RP set entry
Total 1 RP entry

Group(s): 224.0.0.0/4
RP count: 1
RP: 192.168.1.254
Info source: 192.168.1.254, via bootstrap, priority 192
Up time: 00:00:16
Expiry time: 00:02:14
```

---

## Note

- Device 1 and Device 2 are viewed the same way as Device 3, and the viewing process is omitted.
- 

Step 5: Configure PIM and BFD linkage on Device 2 and Device 3.

#Configure Device2.

```
Device2(config)#interface vlan 5
Device2(config-if-vlan5)#ip pim bfd
Device2(config-if-vlan5)#exit
```

#Configure Device3.

```
Device3(config)#interface vlan 4
Device3(config-if-vlan4)#ip pim bfd
Device3(config-if-vlan4)#exit
```

#View the BFD session information of Device 3.

```
Device3#show bfd session detail
Total session number: 1
OurAddr  NeighAddr      LD/RD      State  Holddown  Interface
4.0.0.2  4.0.0.1         5/1        UP     5000     vlan4
Type:ipv4 direct
Local State:UP Remote State:UP Up for: 0h:6m:39s Number of times UP:1
Send Interval:1000ms Detection time:3000ms(1000ms*3)
Local Diag:0 Demand mode:0 Poll bit:0
MinTxInt:1000 MinRxInt:1000 Multiplier:5
Remote MinTxInt:10 Remote MinRxInt:10 Remote Multiplier:3
Registered protocols:PIM
```

Agent session info:

Sender:slot 2 Recver:slot 2

#It is indicated that PIM is successfully associated with BFD.



- Device 2 is viewed the same way as Device 3, and the viewing process is omitted.
- 

Step 6: Check the result.

#Receiver sends an IGMPv2 membership report to join the multicast group 225.1.1.1. Source sends the multicast service packet of the multicast group 225.1.1.1.

#View the multicast membership tables on Device 2 and Device 3, respectively.

```
Device2#show ip igmp groups
```

```
IGMP Connected Group Membership
```

```
Total 1 groups
```

Group Address	Interface	Uptime	Expires	Last Reporter	V1 Expires	V2 Expires
225.1.1.1	vlan5	00:00:56	00:03:25	4.0.0.3	stopped	

```
Device3#show ip igmp groups
```

```
IGMP Connected Group Membership
```

```
Total 1 groups
```

Group Address	Interface	Uptime	Expires	Last Reporter	V1 Expires	V2 Expires
225.1.1.1	vlan4	00:00:02	00:04:17	4.0.0.3	stopped	

#View the PIM-SM multicast routing tables on Device 2 and Device 3, respectively.

```
Device2#show ip pim mroute
```

```
IP Multicast Routing Table:
```

```
PIM VRF Name: Default
```

```
Total 0 (*,*,RP) entry
```

```
Total 1 (*,G) entry
```

```
Total 0 (S,G) entry
```

```
Total 0 (S,G,rpt) entry
```

```
Total 0 FCR entry
```

```
Up timer/Expiry timer
```

(\* , 225.1.1.1)

Up time: 00:04:27

RP: 192.168.1.254

RPF nbr: 0.0.0.0

RPF idx: None

Flags:

Upstream State: NOT JOINED

Local interface list:

vlan5

Joined interface list:

Asserted interface list:

Device3#show ip pim mroute

IP Multicast Routing Table:

PIM VRF Name: Default

Total 0 (\* ,\*,RP) entry

Total 1 (\* ,G) entry

Total 1 (S,G) entry

Total 1 (S,G,rpt) entry

Total 0 FCR entry

Up timer/Expiry timer

(\* , 225.1.1.1)

Up time: 00:02:10

RP: 192.168.1.254

RPF nbr: 2.0.0.1

RPF idx: vlan3

Flags:

JOIN DESIRED

Upstream State: JOINED

Local interface list:

vlan4

Joined interface list:

Asserted interface list:

(192.168.1.1, 225.1.1.1)

```
Up time: 00:00:37
KAT time: 00:02:53
RPF nbr: 2.0.0.1
RPF idx: vlan3
SPT bit: TRUE
Flags:
  JOIN DESIRED
Upstream State: JOINED
Local interface list:
Joined interface list:
Asserted interface list:
Outgoing interface list:
  vlan4
Packet count 0
```

```
(192.168.1.1, 225.1.1.1, rpt)
```

```
Up time: 00:00:37
RP: 192.168.1.254
Flags:
  RPT JOIN DESIRED
  RPF SGRPT XG EQUAL
Upstream State: NOT PRUNED
Local interface list:
Pruned interface list:
Outgoing interface list
```

#It is indicated that the upstream state of the PIM-SM multicast routing table of Device 2 is NOT JOINED, the upstream state of the multicast routing of Device 3 is JOINED, and the multicast service packets are forwarded to Receiver via Device 3.

#When the line between Device 3 and Receiver fails, BFD will quickly detect the failure and notify the PIM-SM protocol, and Device 2 will quickly switches to the receiver DR.

#View the PIM-SM neighbor information, BFD session information, and PIM-SM multicast routing table of Device 2.

```
Device2#show ip pim neighbor
PIM Neighbor Table:
PIM VRF Name: Default
Total 1 Neighbor entry
```

Neighbor Address	Interface	Uptime/Expires	Ver	DR Priority/Mode
3.0.0.1	vlan4	01:12:27/00:01:31	v2	1 /

Device2#show bfd session detail

Total session number: 0

Device2#show ip pim mroute

IP Multicast Routing Table:

PIM VRF Name: Default

Total 0 (\*,\*,RP) entry

Total 1 (\*,G) entry

Total 1 (S,G) entry

Total 1 (S,G,rpt) entry

Total 0 FCR entry

Up timer/Expiry timer

(\*, 225.1.1.1)

Up time: 00:01:03

RP: 192.168.1.254

RPF nbr: 3.0.0.1

RPF idx: vlan4

Flags:

JOIN DESIRED

Upstream State: JOINED

Local interface list:

vlan5

Joined interface list:

Asserted interface list:

(192.168.1.1, 225.1.1.1)

Up time: 00:00:42

KAT time: 00:02:48

RPF nbr: 3.0.0.1

RPF idx: vlan4

SPT bit: TRUE

Flags:  
JOIN DESIRED  
Upstream State: JOINED  
Local interface list:  
Joined interface list:  
Asserted interface list:  
Outgoing interface list:  
vlan5  
Packet count 0

(192.168.1.1, 225.1.1.1, rpt)

Up time: 00:00:42

RP: 192.168.1.254

Flags:  
RPT JOIN DESIRED  
RPF SGRPT XG EQUAL  
Upstream State: NOT PRUNED  
Local interface list:  
Pruned interface list:  
Outgoing interface list:

### #View the PIM-SM neighbors, BFD sessions and multicast routing table of Device 3.

Device3#show ip pim neighbor

PIM Neighbor Table:

PIM VRF Name: Default

Total 1 Neighbor entry

Neighbor Address	Interface	Uptime/Expires	Ver	DR	Priority/Mode
2.0.0.1	vlan3	00:12:27/00:01:20	v2	1	/

Device3#show bfd session detail

Total session number: 0

Device3#show ip pim mroute

IP Multicast Routing Table:

PIM VRF Name: Default

Total 0 (\*,\*,RP) entry

Total 0 (\*,G) entry

Total 0(S,G) entry  
 Total 0 (S,G,rpt) entry  
 Total 0 FCR entry  
 Up timer/Expiry timer

#It is indicated that after the receiver DR Device 3 fails, the BFD session responds immediately, Device 2 switches to the receiver DR, and multicast service packets are forwarded to Receiver via Device 2.

---

## Note

- BFD and PIM linkage is also applicable to the scenario of Assert election on the shared network segment. When the Assert Winner interface malfunctions, Assert Loser can respond quickly to resume forwarding of multicast packets.
- 

### 70.3.5 Configure RPF Routing Switching Convergence with PIM-SM and BFD

#### Linkage

#### Network Requirements

- The PIM-SM protocol runs on the entire network.
- Device 2 is C-BSR and C-RP.
- The entire network uses OSPF to allow for interaction of unicast routing.
- The PIM BFD and OSPF BFD detection function is enabled on the line between Device 1 and Device 3. After the line fails, BFD can quickly detect the failure and notify the PIM and OSPF protocols, so that the RPF neighbor from Device 3 to the multicast source can be quickly switched to Device 2.

#### Network Topology

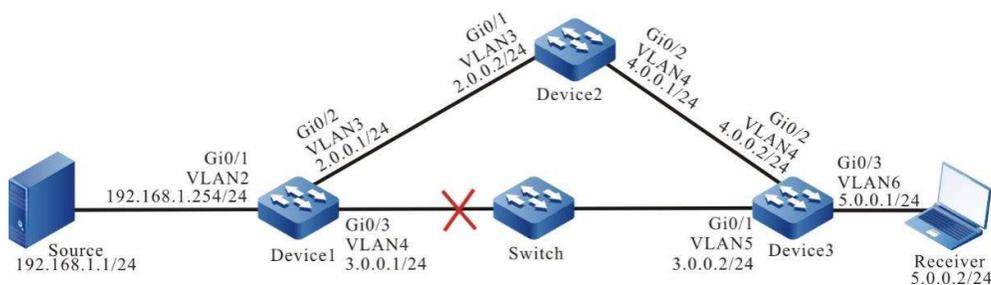


Figure 70-5 Network Topology for Configuring RPF Routing Switching with PIM-SM and BFD Linkage

## Configuration Steps

Step 1: Configure IP addresses for the interfaces (omitted).

Step 2: Enable the unicast routing protocol OSPF, so that all devices in the network can communicate with each other.

### #Configure Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 3.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 192.168.1.0 0.0.0.255 area 0
Device1(config-ospf)#exit
```

### #Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#network 4.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#exit
```

### #Configure Device3.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#network 3.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 4.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 5.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#exit
```

### #View the unicast routing table of Device 3.

```
Device3#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNRP, B - BGP, i-ISIS

Gateway of last resort is not set

C 3.0.0.0/24 is directly connected, 00:01:40, vlan5
C 4.0.0.0/24 is directly connected, 00:00:46, vlan4
C 5.0.0.0/24 is directly connected, 03:45:18, vlan6
```

- C 127.0.0.0/8 is directly connected, 2d:08:42:01, lo0
- O 192.168.1.0/24 [110/2] via 3.0.0.1, 00:01:29, vlan5
- O 2.0.0.0/24 [110/2] via 4.0.0.1, 00:01:29, vlan4  
[110/2] via 3.0.0.1, 00:01:29, vlan5

---

## Note

- Device1 and Device2 are checked in the same way as Device3, the process of which is omitted.
- 

Step 3: Enable multicast forwarding globally, and enable the multicast protocol PIM-SM on the interfaces.

### #Configure Device1.

Enable multicast forwarding globally and enable the multicast protocol PIM-SM on related interfaces.

```
Device1(config)#ip multicast-routing
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#ip pim sparse-mode
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan 3
Device1(config-if-vlan3)#ip pim sparse-mode
Device1(config-if-vlan3)#exit
Device1(config)#interface vlan 4
Device1(config-if-vlan4)#ip pim sparse-mode
Device1(config-if-vlan4)#exit
```

### #Configure Device2.

Enable multicast forwarding globally and enable the multicast protocol PIM-SM on related interfaces.

```
Device2(config)#ip multicast-routing
Device2(config)#interface vlan 3
Device2(config-if-vlan3)#ip pim sparse-mode
Device2(config-if-vlan3)#exit
Device2(config)#interface vlan 4
Device2(config-if-vlan4)#ip pim sparse-mode
Device2(config-if-vlan4)#exit
```

### #Configure Device3.

Enable multicast forwarding globally and enable the multicast protocol PIM-SM on related interfaces.

```
Device3(config)#ip multicast-routing
Device3(config)#interface vlan 4
Device3(config-if-vlan4)#ip pim sparse-mode
Device3(config-if-vlan4)#exit
Device3(config)#interface vlan 6
Device3(config-if-vlan6)#ip pim sparse-mode
Device3(config-if-vlan6)#exit
Device3(config)#interface vlan 5
Device3(config-if-vlan5)#ip pim sparse-mode
Device3(config-if-vlan5)#exit
```

#View, for Device 3, interface information with PIM-SM protocol enabled and PIM-SM neighbor information.

```
Device3#show ip pim interface
PIM Interface Table:
PIM VRF Name: Default
Total 3 Interface entries
Total 0 External Interface entry
Total 0 Sparse-Dense Mode Interface entry
```

Address	Interface	VIF Index	Ver/ Mode	VIF Flag	Nbr Count	DR	DR	BSR	CISCO	Neighbor
					Pri			Border	Neighbor	Filter
4.0.0.2	vlan4	0	v2/S	UP	1 1	4.0.0.2		FALSE	FALSE	
5.0.0.1	vlan6	2	v2/S	UP	0 1	5.0.0.1		FALSE	FALSE	
3.0.0.2	vlan5	3	v2/S	UP	1 1	3.0.0.2		FALSE	FALSE	

```
Device3#show ip pim neighbor
PIM Neighbor Table:
PIM VRF Name: Default
Total 2 Neighbor entries
```

Neighbor Address	Interface	Uptime/Expires	Ver	DR
		Priority/Mode		
4.0.0.1	vlan4	00:05:26/00:01:20	v2	1 /
3.0.0.1	vlan5	00:03:51/00:01:24	v2	1 /

Step 4: Configure C-BSR and C-RP.

#Configure Device2.

Configure vlan 3 of Device 2 as C-BSR and C-RP of the entire network. The range of multicast groups served by C-RP is 224.0.0.0/8.

```
Device2(config)#ip pim bsr-candidate vlan 3
```

```
Device2(config)#ip pim rp-candidate vlan 3
```

#View the BSR and RP information of Device 3.

```
Device3#show ip pim bsr-router
```

```
PIMv2 Bootstrap information
```

```
PIM VRF Name: Default
```

```
BSR address: 2.0.0.2
```

```
BSR Priority: 0
```

```
Hash mask length: 10
```

```
Up time: 00:02:56
```

```
Expiry time: 00:01:14
```

```
Role: Non-candidate BSR
```

```
State: Accept Preferred
```

```
Device3#show ip pim rp mapping
```

```
PIM Group-to-RP Mappings Table:
```

```
PIM VRF Name: Default
```

```
Total 1 RP set entry
```

```
Total 1 RP entry
```

```
Group(s): 224.0.0.0/4
```

```
RP count: 1
```

```
RP: 2.0.0.2
```

```
Info source: 2.0.0.2, via bootstrap, priority 192
```

```
Up time: 00:02:58
```

```
Expiry time: 00:01:32
```

Step 5: Configure PIM, OSPF, and BFD linkage on Device 1 and Device 3.

#Configure Device1.

```
Device1(config)#interface vlan 4
```

```
Device1(config-if-vlan4)#ip pim bfd
```

```
Device1(config-if-vlan4)#ip ospf bfd
```

```
Device1(config-if-vlan4)#exit
```

### #Configure Device3.

```
Device3(config)#interface vlan 5
Device3(config-if-vlan5)#ip pim bfd
Device3(config-if-vlan5)#ip ospf bfd
Device3(config-if-vlan5)#exit
```

### #View the BFD session information of Device 3.

```
Device3#show bfd session detail
Total session number: 1
OurAddr  NeighAddr  LD/RD      State  Holddown  Interface
3.0.0.2  3.0.0.1     5/2       UP     5000     vlan5
Type:ipv4 direct
Local State:UP Remote State:UP Up for: 0h:2m:35s Number of times UP:1
Send Interval:1000ms Detection time:5000ms(1000ms*5)
Local Diag:0 Demand mode:0 Poll bit:0
MinTxInt:1000 MinRxInt:1000 Multiplier:5
Remote MinTxInt:1000 Remote MinRxInt:1000 Remote Multiplier:5
Registered protocols:OSPF PIM
Agent session info:
Sender:slot 1 Recver:slot 1
```

#It is indicated that the BFD session between Device 1 and Device 3 is established normally, and the OSPF and PIM protocols are successfully associated.

---

## Note

- Device1 is checked in the same way as that of Device3, the process of which is omitted.
- 

Step 6: Check the result.

#Receiver sends an IGMPv2 membership report to join the multicast group 225.1.1.1. Source sends the multicast service packet of the multicast group 225.1.1.1.

#View the multicast membership table of Device 3.

```
Device3#show ip igmp groups
IGMP Connected Group Membership
Total 1 groups
Group Address  Interface          Uptime  Expires  Last Reporter  V1 Expires  V2 Expires
225.1.1.1     vlan6              02:55:24 00:04:18 5.0.0.3        stopped
```

### #View the PIM-SM multicast routing table of Device 3.

```
Device3#show ip pim mroute
```

```
IP Multicast Routing Table:
```

```
PIM VRF Name: Default
```

```
Total 0 (*,*,RP) entry
```

```
Total 1 (*,G) entry
```

```
Total 1 (S,G) entry
```

```
Total 1 (S,G,rpt) entry
```

```
Total 0 FCR entry
```

```
Up timer/Expiry timer
```

```
(*, 225.1.1.1)
```

```
Up time: 02:57:30
```

```
RP: 2.0.0.2
```

```
RPF nbr: 4.0.0.1
```

```
RPF idx: vlan4
```

```
Flags:
```

```
JOIN DESIRED
```

```
Upstream State: JOINED
```

```
Local interface list:
```

```
    vlan6
```

```
Joined interface list:
```

```
Asserted interface list:
```

```
(192.168.1.1, 225.1.1.1)
```

```
Up time: 00:12:58
```

```
KAT time: 00:03:03
```

```
RPF nbr: 3.0.0.1
```

```
RPF idx: vlan5
```

```
SPT bit: TRUE
```

```
Flags:
```

```
JOIN DESIRED
```

```
Upstream State: JOINED
```

```
Local interface list:
```

```
Joined interface list:
```

```
Asserted interface list:
```

Outgoing interface list:

vlan6

Packet count 620657

(192.168.1.1, 225.1.1.1, rpt)

Up time: 00:12:58

RP: 2.0.0.2

Flags:

RPT JOIN DESIRED

RPF SGRPT XG EQUAL

Upstream State: NOT PRUNED

Local interface list:

Pruned interface list:

Outgoing interface list:

#It is indicated that the RPF neighbor from Device 3 to the multicast source is Device 1, and the incoming interface for multicast service packets is vlan 5.

#When the line between Device 1 and Device 3 fails, BFD will quickly detect the failure and notify the OSPF and PIM protocols, OSPF will switch the routing to Device 2 for communication and notify the PIM protocol that the unicast routing has changed, and the PIM protocol will quickly switch to the RPF neighbor of the multicast source.

#View the PIM-SM neighbor and multicast group routing table of Device 3.

```
Device3#show ip pim neighbor
```

PIM Neighbor Table:

PIM VRF Name: Default

Total 1 Neighbor entry

Neighbor	Interface	Uptime/Expires	Ver	DR
Address			Priority/Mode	
4.0.0.1	vlan4	00:34:40/00:01:37	v2	1 /

```
Device3#show ip pim mroute
```

IP Multicast Routing Table:

PIM VRF Name: Default

Total 0 (\*,\*,RP) entry

Total 1 (\*,G) entry

Total 1 (S,G) entry

Total 1 (S,G,rpt) entry

Total 0 FCR entry  
Up timer/Expiry timer

(\*, 225.1.1.1)

Up time: 03:07:04

RP: 2.0.0.2

RPF nbr: 4.0.0.1

RPF idx: vlan4

Flags:

JOIN DESIRED

Upstream State: JOINED

Local interface list:

vlan6

Joined interface list:

Asserted interface list:

(192.168.1.1, 225.1.1.1)

Up time: 00:22:32

KAT time: 00:03:29

RPF nbr: 4.0.0.1

RPF idx: vlan4

SPT bit: TRUE

Flags:

JOIN DESIRED

Upstream State: JOINED

Local interface list:

Joined interface list:

Asserted interface list:

Outgoing interface list:

vlan6

Packet count 1127697

(192.168.1.1, 225.1.1.1, rpt)

Up time: 00:22:32

RP:2.0.0.2

Flags:

RPT JOIN DESIRED  
RPF SGRPT XG EQUAL  
Upstream State: NOT PRUNED  
Local interface list:  
Pruned interface list:  
Outgoing interface list:  
vlan6

#It is indicated that the RPF neighbor from Device 3 to the multicast source is Device 2, and the incoming interface for multicast service packets is vlan 4.

---

 **Note**

- Since the RPF routing convergence with PIM and BFD linkage also depends on the convergence speed of unicast routing, BFD also needs to be linked with the related unicast routing protocol OSPF.
-



# 71 MSDP

---

## 71.1 Overview

RP in the PIM-SM network only knows the multicast source information in the multicast domain to which it belongs. However, in practical applications, the entire network is usually divided into multiple multicast domains. In this case, RP in the domain cannot know the multicast source information outside the domain, and the receiver cannot receive multicast data packets from other domains.

MSDP (Multicast Source Discovery Protocol) provides a multicast cross-domain solution. The MSDP mechanism allows for transmission of the multicast source information of the local multicast domain to RP of another multicast domain, and RPs of other multicast domains can join the multicast source of the local multicast domain and establish a multicast distribution tree, thereby allowing for cross-domain transmission of multicast data packets.

## 71.2 MSDP Function Configuration

Table 71-1 MSDP Function Configuration List

Configuration Task	
Configure basic functions of MSDP	Configure MSDP peer
	Shut down MSDP peer
Configure MSDP peer connection	Configure default MSDP peer
	Configure MSDP mesh group
Configure SA packet	Configure SA request packet
	Configure SA packet filtering policy



- 
- The L3 Ethernet interface does not support the MSDP function.
- 

### 71.2.1 Configure MSDP peer

MSDP peer-to-peer connections are established between various multicast domains through MSDP peers to form an "MSDP connected graph" with the domains connected to each other. When the MSDP peer of a certain domain senses a new multicast source, it will encapsulate the new multicast source information in the SA (Source-Active) packet and send it to all remote peers with the MSDP peer-to-peer connections established. After the MSDP peer receives the SA packet, the SA packet that passed an RPF (Reverse Path Forwarding) check will be forwarded. Through the relay between the MSDP peers, the SA packet sent by a certain RP can be transferred to all other RPs, and the multicast source information is finally shared among the multicast domains.

MSDP peers use TCP as their transmission protocol, and use the reliability of TCP to ensure that MSDP protocol packets can be correctly transmitted to the remote peers.

#### Configuration Condition

Before configuring MSDP, do the following:

- Configure the network layer address of the interface so that all neighbor nodes are reachable at the network layer;
- Configure any unicast routing protocol to achieve reachable routes within the domain;
- Configure the PIM-SM protocol to implement intra-domain multicast.

#### Configure MSDP peer

The local device establishes an MSDP peer-to-peer connection with the specified remote device, and the remote device must also specify the local end as the MSDP peer to successfully establish the peer-to-peer connection. After the peer-to-peer connection is successfully established, the peers exchange MSDP protocol packets through this connection.

Table 71-2 Configuring MSDP Peer

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure MSDP peer	<b>ip msdp [ vrf vrf-name ] peer peer-ip-address [ connect-source interface-name ] [ remote-as as-number-value ]</b>	Mandatory By default, no MSDP peer is configured

---

### Note

- When configuring the first MSDP peer, the MSDP protocol is automatically enabled.
- 

### Shut down MSDP peer

The administrator can use this command to shut down the specified MSDP peer-to-peer connection according to the network needs. After the MSDP peer-to-peer connection is shut down, the exchange of the MSDP protocol packets between the MSDP peers will be stopped.

Table 71-3 Shutting Down MSDP Peer

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Shut down MSDP peer	<b>ip msdp [ vrf vrf-name ] shutdown peer-ip-address</b>	Mandatory By default, no MSDP peer is shut down

## 71.2.2 Configure MSDP peer connection

After the device receives an SA packet, it will perform an RPF check. The packet that passed the check will be forwarded to other peers that have established the peer-to-peer connection. If it fails the RPF check, the packet will be dropped.

For the default peers, the mesh group can omit the RPF check for SA packets between the specified peers.

### Configuration Condition

Before configuring MSDP, do the following:

- Configure the network layer address of the interface so that all neighbor nodes are reachable at the network layer;
- Configure any unicast routing protocol to achieve reachable routes within the domain;
- Configure the PIM-SM protocol to implement intra-domain multicast;
- Configure MSDP peers.

### Configure default MSDP peer

When specifying the default MSDP peer, you can configure the RP range. When receiving an SA packet from the default peer, if RP in the packet falls within the allowable range, the RPF check will not be performed. Otherwise the RPF check will be performed on RP in the packet.

Table 71-4 Configuring Default MSDP Peer

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure default MSDP peer	<b>ip msdp [ vrf vrf-name ] default-peer peer-ip-address [ prefix-list prefix-list-name ]</b>	Mandatory By default, no MSDP default peer is configured

### Configure MSDP mesh group

When the device receives an SA packet from the peer in the group, it directly passes the RPF check and does not forward the SA packet to other peers in the group, but only forwards it to peers outside the group. This can reduce the burden on the device and avoid repeated forwarding of SA packets, thereby saving network bandwidth;

Table 71-5 Configuring MSDP Mesh Group

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure MSDP mesh group	<b>ip msdp [ vrf vrf-name ] mesh-group mesh-group-name peer-ip-address</b>	Mandatory By default, no peer joins the mesh group

### 71.2.3 Configure SA packet

#### Configuration Condition

Before configuring MSDP, do the following:

- Configure the network layer address of the interface so that all neighbor nodes are reachable at the network layer;
- Configure any unicast routing protocol to achieve reachable routes within the domain;
- Configure the PIM-SM protocol to implement intra-domain multicast;
- Configure MSDP peers.

#### Configure SA request packet

After the device is configured to send an SA request packet, when the device receives a new multicast group join packet, it will immediately send the SA request packet to the MSDP peer, thereby reducing the delay in joining the multicast group.

Some RPs do not want to be known by receivers of other unrecognized multicast domains. The filtering policy for SA request packets can be configured on all peers in the multicast domain to which the RP belongs, and only SA request packets from the peer allowed by the policy will be responded.

Table 71-6 Configuring SA Request Packet

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure to send SA request packet	<b>ip msdp [ vrf vrf-name ] sa-request peer-ip-address</b>	Mandatory By default, when the device receives a new multicast group join packet, it will not send an SA request packet to the MSDP peer, but will wait for the SA packet in the next period
Configure filtering policy for receiving SA request packets	<b>ip msdp [ vrf vrf-name ] filter-sa-request peer-ip-address [ list access-list-number   access-list-name ]</b>	Mandatory By default, SA request packets are not filtered

 **Note**

- The command **ip msdp filter-sa-request** only supports standard ACL.

**Configure SA packet filtering policy**

Generally, the MSDP peer accepts the SA packets from all peers that pass the RPF check, and forward them to all peers outside the mesh group. The user can configure the SA packet filtering policy on peers as needed to control the SA packets from or sent to the specified peer. When receiving or forwarding the SA packet, the device filters the multicast source group and RP of the SA packet.

Table 71-7 Configuring SA Packet Filtering Policy

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure SA packet filtering policy	<b>ip msdp [ vrf vrf-name ] sa-filter { in   out } peer-ip-address [ list { access-list-name   access-list-number } ] [ rp-list { access-list-name   access-list-number } ]</b>	Mandatory By default, SA packets are not filtered

### Note

- The parameter **list** of the command **ip msdp sa-filter** only supports extended ACL.
- The parameter **rp-list** of the command **ip msdp sa-filter** only supports standard ACL.

## 71.2.4 MSDP Monitoring and Maintaining

Table 71-8 MSDP Monitoring and Maintaining

Command	Description
<b>clear ip msdp [ vrf vrf-name ] peer [ peer-ip-address ]</b>	Clear MSDP peer information
<b>clear ip msdp [ vrf vrf-name ] sa-cache [ group-ip-address ]</b>	Clear SA cache information
<b>clear ip msdp [ vrf vrf-name ] statistics [ peer-ip-address ]</b>	Clear MSDP peer statistics
<b>show ip msdp [ vrf vrf-name ] count [ as-number-value ]</b>	Show SA information received by MSDP from AS domain

Command	Description
<b>show ip msdp</b> [ vrf <i>vrf-name</i> ] <b>peer</b> [ <i>peer-ip-address</i> [ <b>accepted-SAs</b>   <b>advertised-SAs</b> ] ]	Show MSDP peer information
<b>show ip msdp</b> [ vrf <i>vrf-name</i> ] <b>rpf</b> [ <i>peer-ip-address</i> ]	Show MSDP next hop routing information
<b>show ip msdp</b> [ vrf <i>vrf-name</i> ] <b>sa-cache</b> [ <i>group-ip-address</i> [ <i>source-ip-address</i> ] ] [ <i>as-number-value</i> ]	Show MSDP SA cache information
<b>show ip msdp</b> [ vrf <i>vrf-name</i> ] <b>summary</b>	Show MSDP peer summary

## 71.3 MSDP Typical Configuration Example

### 71.3.1 Configure PIM-SM Inter-domain Multicast

#### Network Requirements

- The entire network includes two autonomous systems: AS100 and AS200. The BGP protocol is run between ASes, and MBGP is used for multicast routing exchanging. The OSPF protocol is run within the AS for routing exchanging.
- The multicast domain PIM-SM1 is located in AS100, and the multicast domain PIM-SM2 is located in AS200. Source is one multicast source of PIM-SM1, and Receiver is one receiver of PIM-SM2.
- Loopback 1 of Device 2 is C-BSR of PIM-SM1, Loopback 0 is C-RP of PIM-SM1, Loopback 1 of Device 3 is C-BSR of PIM-SM2, and Loopback 0 is C-RP of PIM-SM2.
- An MSDP peer-to-peer connection is established between Device 2 and Device 3 to allow for the cross-domain forwarding of multicast service packets, so that Receiver can receive the multicast service packets sent by Source.

#### Network Topology

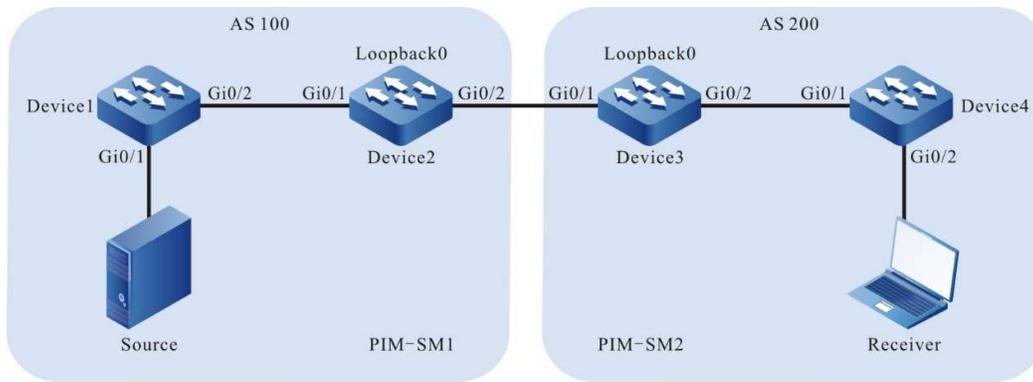


Figure 71-1 Network Topology for Configuring PIM-SM Inter-domain Multicast

of equipment	Interface	VLAN	IP address
Device1	Gi0/1	2	10.1.1.1/24
	Gi0/2	3	10.1.2.1/24
Device2	Gi0/1	3	10.1.2.2/24
	Gi0/2	4	10.1.3.1/24
	Loopback0		11.11.11.11/32
	Loopback1		12.12.12.12/32
Device3	Gi0/1	4	10.1.3.2/24
	Gi0/2	5	10.1.4.1/24
	Loopback0		22.22.22.22/32
	Loopback1		23.23.23.23/32
Device4	Gi0/1	5	10.1.4.2/24
	Gi0/2	6	10.1.5.1/24
Source			10.1.1.2/24

## Configuration Steps

- Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)
- Step 2: Configure IP addresses for the ports. (Omitted)
- Step 3: Configure OSPF so that all devices in each AS domain can communicate with each other.

### #Configure Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#network 10.1.1.0 0.0.0.255 area 0
Device1(config-ospf)#network 10.1.2.0 0.0.0.255 area 0
Device1(config-ospf)#exit
```

### #Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 10.1.2.0 0.0.0.255 area 0
Device2(config-ospf)#network 11.11.11.11 0.0.0.0 area 0
Device2(config-ospf)#network 12.12.12.12 0.0.0.0 area 0
Device2(config-ospf)#exit
```

### #Configure Device3.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#network 10.1.4.0 0.0.0.255 area 0
Device3(config-ospf)#network 22.22.22.22 0.0.0.0 area 0
Device3(config-ospf)#network 23.23.23.23 0.0.0.0 area 0
Device3(config-ospf)#exit
```

### #Configure Device4.

```
Device4#configure terminal
Device4(config)#router ospf 100
Device4(config-ospf)#network 10.1.4.0 0.0.0.255 area 0
Device4(config-ospf)#network 10.1.5.0 0.0.0.255 area 0
Device4(config-ospf)#exit
```

### #View the routing table of Device1.

```
Device1#show ip route
```

```
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
```

```
D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS
```

```
Gateway of last resort is not set
```

```
C 10.1.1.0/24 is directly connected, 00:05:44, vlan2
```

```
C 10.1.2.0/24 is directly connected, 22:24:35, vlan3
```

```
O 11.11.11.11/32 [110/2] via 10.1.2.2, 01:21:25, vlan3
```

```
O 12.12.12.12/32 [110/2] via 10.1.2.2, 01:19:25, vlan3
```

#### #View the routing table of Device 4.

```
Device4#show ip route
```

```
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
```

```
D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS
```

```
Gateway of last resort is not set
```

```
C 10.1.4.0/24 is directly connected, 22:41:14, vlan5
```

```
C 10.1.5.0/24 is directly connected, 00:08:11, vlan6
```

```
O 22.22.22.22/32 [110/2] via 10.1.4.1, 01:23:33, vlan5
```

```
O 23.23.23.23/32 [110/2] via 10.1.4.1, 01:19:33, vlan5
```

It is indicated that Device 1 and Device 4 have only learned the routing of their AS domains.

---

### Note

- Device 2 and Device 3 are viewed the same way as Device 1, and Device 4, and the viewing process is omitted.
- 

Step 4: Enable multicast forwarding globally, enable the multicast protocol PIM-SM on the interfaces, and configure C-BSR and C-RP.

#Configure Device 1. Enable multicast forwarding globally, and enable the multicast protocol PIM-SM on the interfaces.

```
Device1(config)#ip multicast-routing
```

```
Device1(config)#interface vlan 2
```

```
Device1(config-if-vlan2)#ip pim sparse-mode
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan 3
Device1(config-if-vlan3)#ip pim sparse-mode
Device1(config-if-vlan3)#exit
```

**#Configure Device 2. Enable multicast forwarding globally, enable the multicast protocol PIM-SM on the interfaces, and configure Loopback 1 as C-BSR, Loopback 0 as C-RP. The range of multicast groups served by C-RP is 224.0.0.0/4.**

```
Device2(config)#ip multicast-routing
Device2(config)#interface loopback 0
Device2(config-if-loopback0)#ip pim sparse-mode
Device2(config-if-loopback0)#exit
Device2(config)#interface loopback 1
Device2(config-if-loopback1)#ip pim sparse-mode
Device2(config-if-loopback1)#exit
Device2(config)#interface vlan 3
Device2(config-if-vlan3)#ip pim sparse-mode
Device2(config-if-vlan3)#exit
Device2(config)#interface vlan 4
Device2(config-if-vlan4)#ip pim sparse-mode
Device2(config-if-vlan4)#exit
Device2(config)#ip pim bsr-candidate loopback1
Device2(config)#ip pim rp-candidate loopback0
```

**#Configure Device 3. Enable multicast forwarding globally, enable the multicast protocol PIM-SM on the interfaces, and configure Loopback 1 as C-BSR, Loopback 0 as C-RP. The range of multicast groups served by C-RP is 224.0.0.0/4.**

```
Device3(config)#ip multicast-routing
Device3(config)#interface loopback 0
Device3(config-if-loopback0)#ip pim sparse-mode
Device3(config-if-loopback0)#exit
Device3(config)#interface loopback 1
Device3(config-if-loopback1)#ip pim sparse-mode
Device3(config-if-loopback1)#exit
Device3(config)#interface vlan 4
Device3(config-if-vlan4)#ip pim sparse-mode
Device3(config-if-vlan4)#exit
Device3(config)#interface vlan 5
Device3(config-if-vlan5)#ip pim sparse-mode
```

```

Device3(config-if-vlan5)#exit
Device3(config)#ip pim bsr-candidate loopback 1
Device3(config)#ip pim rp-candidate loopback0

```

#Configure Device 4. Enable multicast forwarding globally, and enable the multicast protocol PIM-SM on the interfaces.

```

Device4(config)#ip multicast-routing
Device4(config)#interface vlan 5
Device4(config-if-vlan5)#ip pim sparse-mode
Device4(config-if-vlan5)#exit
Device4(config)#interface vlan 6
Device4(config-if-vlan6)#ip pim sparse-mode
Device4(config-if-vlan6)#exit

```

#View, for Device 4, interface information with PIM-SM protocol enabled and PIM-SM neighbor information.

```

Device4#show ip pim interface
PIM Interface Table:
PIM VRF Name: Default
Total 3 Interface entries
Total 0 External Interface entry
Total 0 Sparse-Dense Mode Interface entry

```

Address	Interface	VIF Index	Ver/ Mode	VIF Flag	Nbr Count	DR Pri	DR	BSR Border	CISCO Neighbor Filter	Neighbor
10.1.4.2	register_vif0	1	v2/S	UP						
10.1.4.2	vlan5	0	v2/S	UP	1 1	10.1.4.2		FALSE	FALSE	
10.1.5.1	vlan6	2	v2/S	UP	0 1	10.1.5.1		FALSE	FALSE	

```

Device4#show ip pim neighbor
PIM Neighbor Table:
PIM VRF Name: Default
Total 1 Neighbor entry

```

Neighbor Address	Interface	Uptime/Expires	Ver	DR
10.1.4.1	vlan5	23:03:12/00:01:20	v2	1 /

---

 **Note**

- Device 1, Device 2, and Device 3 are viewed the same way as Device 4, and the viewing process is omitted.
- 

#### #View the BSR and RP information of Device 4.

```
Device4#show ip pim bsr-router
```

```
PIMv2 Bootstrap information
```

```
PIM VRF Name: Default
```

```
BSR address: 23.23.23.23
```

```
BSR Priority: 0
```

```
Hash mask length: 10
```

```
Up time: 01:57:44
```

```
Expiry time: 00:01:28
```

```
Role: Non-candidate BSR
```

```
State: Accept Preferred
```

```
Device4#show ip pim rp mapping
```

```
PIM Group-to-RP Mappings Table:
```

```
PIM VRF Name: Default
```

```
Total 1 RP set entry
```

```
Total 1 RP entry
```

```
Group(s): 224.0.0.0/4
```

```
RP count: 1
```

```
RP: 22.22.22.22
```

```
Info source: 23.23.23.23, via bootstrap, priority 192
```

```
Up time: 01:57:45
```

```
Expiry time: 00:01:47
```

#### #View the BSR and RP information of Device 1.

```
Device1#show ip pim bsr-router
```

```
PIMv2 Bootstrap information
```

```
PIM VRF Name: Default
```

```
BSR address: 12.12.12.12
```

```
BSR Priority: 0
```

```
Hash mask length: 10
```

Up time: 02:00:24  
Expiry time: 00:01:44  
Role: Non-candidate BSR  
State: Accept Preferred

Device1#show ip pim rp mapping  
PIM Group-to-RP Mappings Table:  
PIM VRF Name: Default  
Total 1 RP set entry  
Total 1 RP entry

Group(s): 224.0.0.0/4  
RP count: 1  
**RP: 11.11.11.11**  
Info source: 12.12.12.12, via bootstrap, priority 192  
Up time: 02:00:30  
Expiry time: 00:01:58

It is indicated that only the BSR and RP information of the multicast domain to which they belong are present on Device 4 and Device 1.

---

### Note

- Device 2 and Device 3 are viewed the same way as Device 1, and Device 4, and the viewing process is omitted.
- 

Step 5: Configure MP-EBGP. A directly connected EBGP peer is established between Device 2 and Device 3, and multicast routing is exchanged using MBGP.

#Configure Device 2. Configure the EBGP peer directly connected with Device 3, enable Multicast address family, and advertise multicast routing.

```
Device2(config)#router bgp 100
Device2(config-bgp)#neighbor 10.1.3.2 remote-as 200
Device2(config-bgp)#address-family ipv4 multicast
Device2(config-bgp-af)#network 10.1.1.0 255.255.255.0
Device2(config-bgp-af)#network 11.11.11.11 255.255.255.255
```

```
Device2(config-bgp-af)#neighbor 10.1.3.2 activate
Device2(config-bgp-af)#exit-address-family
Device2(config-bgp)#exit
```

#Configure Device 3. Configure the EBGp peer directly connected with Device 2, enable Multicast address family, and advertise multicast routing.

```
Device3(config)#router bgp 200
Device3(config-bgp)#neighbor 10.1.3.1 remote-as 100
Device3(config-bgp)#address-family ipv4 multicast
Device3(config-bgp-af)#network 10.1.5.0 255.255.255.0
Device3(config-bgp-af)#network 22.22.22.22 255.255.255.255
Device3(config-bgp-af)#neighbor 10.1.3.1 activate
Device3(config-bgp-af)#exit-address-family
Device3(config-bgp)#exit
```

#View the BGP neighbor state of Device 3.

```
Device3#show ip bgp summary
BGP router identifier 22.22.22.22, local AS number 200
BGP table version is 2
2 BGP AS-PATH entries
0 BGP community entries

Neighbor      V   AS MsgRcvd MsgSent  TblVer  InQ  OutQ  Up/Down  State/PfxRcd
10.1.3.1     4  100   114   111     2    0   00:35:00    0

Total number of neighbors 1
```

From the case where the content of the State/PfxRcd column is displayed as a digit (from the number of unicast routing prefixes received by the neighbor), It is indicated that Device 3 and Device 2 successfully established the BGP neighbor.

#View the BGP Multicast routing table of Device 3.

```
Device3#show bgp ipv4 multicast
BGP table version is 9, local router ID is 22.22.22.22
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
                S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Network        Next Hop        Metric LocPrf Weight Path
[B]*> 10.1.1.0/24  10.1.3.1         2         0 100 i
[B]*> 10.1.5.0/24  10.1.4.2         2        32768 i
[B]*> 11.11.11.11/32  10.1.3.1         0         0 100 i
```

```
[B]*> 22.22.22.22/32 0.0.0.0 0 32768 i
```

It is indicated that Device 3 has learned Source and RP routing of the multicast domain PIM-SM1, and the next hop is the MSDP peer 10.1.3.1.

---

 **Note**

- Device 2 is viewed the same way as Device 3, and the viewing process is omitted.
- 

Step 6: Configure MSDP.

#Configure Device 2. Configure a MSDP peer-to-peer connection that is directly connected to Device 3; enable the function of actively sending the SA request packet to the specified peer; configure to use RFC3618 rules to perform the RPF check on MSDP packets.

```
Device2(config)#ip msdp peer 10.1.3.2 remote-as 200
```

```
Device2(config)#ip msdp sa-request 10.1.3.2
```

```
Device2(config)#ip msdp rpf rfc3618
```

#Configure Device 3. Configure a MSDP peer-to-peer connection that is directly connected to Device 2; enable the function of actively sending the SA request packet to the specified peer; configure to use RFC3618 rules to perform the RPF check on MSDP packets.

```
Device3(config)#ip msdp peer 10.1.3.1 remote-as 100
```

```
Device3(config)#ip msdp sa-request 10.1.3.1
```

```
Device3(config)#ip msdp rpf rfc3618
```

#View the MSDP peer-to-peer connection status and details of Device 3.

```
Device3#show ip msdp summary
```

```
MSDP Peer Status Summary
```

```
Total 1 Peer entry
```

```
Peer Address  AS  State  Reset  Uptime/Downtime
```

```
10.1.3.1     100  Up    0     02:21:18
```

```
Device3#show ip msdp peer
```

```
MSDP Peer Table:
```

```
Total 1 Peer entry
```

```
MSDP Peer 10.1.3.1, AS 100 (configured AS)
```

```
Connection status:
```

```

State: Established, Resets: 0, Connection source: none configured
Uptime(Downtime): 02:50:00, Message sent/received: 136/161
Connection and counters cleared 02:13:25 ago
Local Address of connection: 10.1.3.2
Remote Address of connection: 10.1.3.1
Local Port: 639, Remote Port: 1179
SA-Requests:
Input filter: none
Sending SA-Requests to peer: enabled
SA:
Input filter: none
Message counters:
RPF Failure count: 0
SA Messages in/out: 47/0
SA Requests in/out: 0/3
SA Responses in/out: 3/0
Data Packets in/out: 0/0

```

It is indicated that Device 3 and Device 2 have successfully established the MSDP peer-to-peer connection.

---

### Note

- Device 2 is viewed the same way as Device 3, and the viewing process is omitted.
- 

Step 7: Check the result.

#Receiver sends an IGMPv2 member report to join the multicast group 225.1.1.1. Source sends the multicast service packet of the multicast group 225.1.1.1.

#View the multicast membership table on Device 4.

```

Device4#show ip igmp groups
IGMP Connected Group Membership
Total 1 groups

```

Group Address	Interface	Uptime	Expires	Last Reporter	V1 Expires	V2 Expires
225.1.1.1	vlan6	00:05:11	00:02:38	10.1.5.2	stopped	

#View the MSDP SA cache information of Device 2.

```
Device2#show ip msdp sa-cache
MSDP Source-Active Cache - 1 entries
(10.1.1.2, 225.1.1.1), RP 11.11.11.11, Originated, 00:11:45/00:05:39
```

It is indicated that the SA packet is generated and cached on Device 2. In the SA packet, the multicast source address is 10.1.1.2, the multicast group address is 225.1.1.1, and the RP address is 11.11.11.11.

#View the MSDP SA cache information and RPF checklist of Device 3.

```
Device3#show ip msdp sa-cache
MSDP Source-Active Cache - 1 entries
(10.1.1.2, 225.1.1.1), RP 11.11.11.11, Recv From Peer 10.1.3.1, 00:08:39/00:05:21
```

```
Device3#show ip msdp rpf
Destination  Nexthop      Nexthop      Nexthop Metric Pref
Address      Address      From          RefCnt
10.1.3.1     0.0.0.0     0.0.0.0      1   10   0
11.11.11.11 10.1.3.1    10.1.3.1     1   0   20
```

It is indicated that Device 3 has received and cached the SA packet. The SA packet came from the peer 10.1.3.1. In the packet, the multicast source address is 10.1.1.2, the multicast group address is 225.1.1.1, and the RP address is 11.11.11.11. The next hop on the best path for Device 3 to reach the source RP (11.11.11.11) is 10.1.3.1.

#View the PIM-SM multicast routing table of Device 3.

```
Device3#show ip pim mroute
IP Multicast Routing Table:
PIM VRF Name: Default
Total 0 (*,*,RP) entry
Total 1 (*,G) entry
Total 1 (S,G) entry
Total 1 (S,G,rpt) entry
Total 0 FCR entry
Up timer/Expiry timer

(*, 225.1.1.1)
Up time: 00:13:57
RP: 22.22.22.22
```

RPF nbr: 0.0.0.0  
RPF idx: None  
Flags:  
JOIN DESIRED  
Upstream State: JOINED  
Local interface list:  
Joined interface list:  
vlan5 00:13:57/00:02:33  
Asserted interface list:

(10.1.1.2, 225.1.1.1)

Up time: 00:13:57  
KAT time: 00:03:28  
RPF nbr: 10.1.3.1  
RPF idx:vlan4  
SPT bit: TRUE

Flags:  
JOIN DESIRED  
Upstream State: JOINED  
Local interface list:  
Joined interface list:  
Asserted interface list:  
Outgoing interface list:  
vlan5  
Packet count 6906038

(10.1.1.2, 225.1.1.1, rpt)

Up time: 00:13:57  
RP: 22.22.22.22  
Flags:  
RPT JOIN DESIRED  
PRUNE DESIRED  
RPF SGRPT XG EQUAL  
Upstream State: PRUNED  
Local interface list:  
Pruned interface list:  
Outgoing interface list:

vlan5

#Receiver can only receive the multicast service packet of the multicast group 225.1.1.1 sent by Source.

---

## Note

- Device 2 is viewed the same way as Device 3, and the viewing process is omitted.
- 

### 71.3.2 Configure Anycast RP

#### Network Requirements

- The PIM-SM protocol runs on the entire PIM multicast domain.
- Loopback 0 interface of Device 3 is C-BSR, and Loopback 1 interface of each of Device 2 and Device 4 is C-RP and has the same IP address.
- Use the IP address of Loopback 0 to establish the MSDP peer-to-peer connection between Device 2 and Device 4.
- Configure multiple RPs with the same address in the domain. Non-RP devices will select the nearest RP for multicast source and receiver management. These RPs exchange multicast source information through MSDP, allowing for interaction of the multicast services of the entire multicast domain. If there is a problem with one RP, its management area will be shared by other RPs.

#### Network Topology

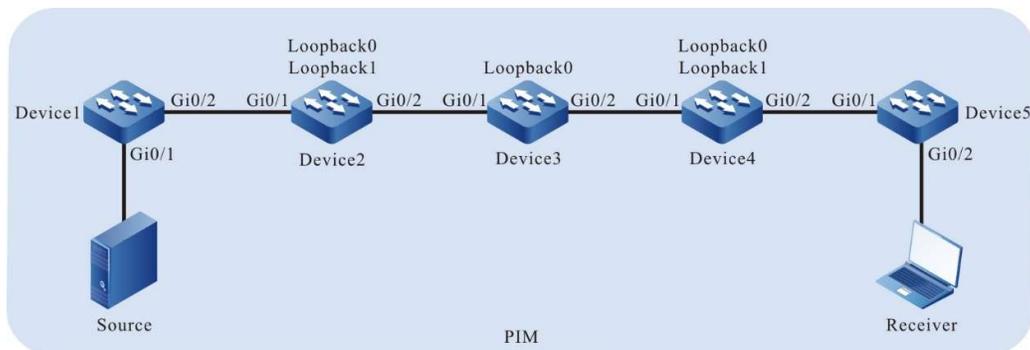


Figure 71-2 Network Topology for Configuring Anycast RP

of equipment	Interface	VLAN	IP address
Device1	Gi0/1	2	10.1.1.1/24
	Gi0/2	3	10.1.2.1/24
Device2	Gi0/1	3	10.1.2.2/24
	Gi0/2	4	10.1.3.1/24
	Loopback0		11.11.11.11/32
	Loopback1		55.55.55.55/32
Device3	Gi0/1	4	10.1.3.2/24
	Gi0/2	5	10.1.4.1/24
	Loopback0		44.44.44.44/32
Device4	Gi0/1	5	10.1.4.2/24
	Gi0/2	6	10.1.5.1/24
	Loopback0		22.22.22.22/32
	Loopback1		55.55.55.55/32
Device5	Gi0/1	6	10.1.5.2/24
	Gi0/2	7	10.1.6.1/24
Source	-		10.1.1.2/24

### Configuration Steps

Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configure IP addresses for the ports. (Omitted)

Step 3: Configure OSPF so that all devices in the network can communicate with each other.

#### #Configure Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#network 10.1.1.0 0.0.0.255 area 0
Device1(config-ospf)#network 10.1.2.0 0.0.0.255 area 0
Device1(config-ospf)#exit
```

#### #Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 10.1.2.0 0.0.0.255 area 0
Device2(config-ospf)#network 10.1.3.0 0.0.0.255 area 0
Device2(config-ospf)#network 11.11.11.11 0.0.0.0 area 0
Device2(config-ospf)#network 55.55.55.55 0.0.0.0 area 0
Device2(config-ospf)#exit
```

#### #Configure Device3.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#network 10.1.3.0 0.0.0.255 area 0
Device3(config-ospf)#network 10.1.4.0 0.0.0.255 area 0
Device3(config-ospf)#network 44.44.44.44 0.0.0.0 area 0
Device3(config-ospf)#exit
```

#### #Configure Device4.

```
Device4#configure terminal
Device4(config)#router ospf 100
Device4(config-ospf)#network 10.1.4.0 0.0.0.255 area 0
Device4(config-ospf)#network 10.1.5.0 0.0.0.255 area 0
Device4(config-ospf)#network 22.22.22.22 0.0.0.0 area 0
Device4(config-ospf)#network 55.55.55.55 0.0.0.0 area 0
Device4(config-ospf)#exit
```

#### #Configure Device5.

```
Device5#configure terminal
Device5(config)#router ospf 100
Device5(config-ospf)#network 10.1.5.0 0.0.0.255 area 0
```

```
Device5(config-ospf)#network 10.1.6.0 0.0.0.255 area 0
```

```
Device5(config-ospf)#exit
```

#View the routing table of Device5.

```
Device5#show ip route
```

Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management

D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

```
Gateway of last resort is not set
```

```
O 10.1.1.0/24 [110/5] via 10.1.5.1, 04:04:37, vlan6
O 10.1.2.0/24 [110/4] via 10.1.5.1, 04:05:13, vlan6
O 10.1.3.0/24 [110/3] via 10.1.5.1, 04:17:36, vlan6
O 10.1.4.0/24 [110/2] via 10.1.5.1, 18:19:08, vlan6
C 10.1.5.0/24 is directly connected, 18:22:13, vlan6
C 10.1.6.0/24 is directly connected, 04:32:51, vlan7
O 11.11.11.11/32 [110/4] via 10.1.5.1, 04:17:36, vlan6
O 22.22.22.22/32 [110/2] via 10.1.5.1, 03:56:25, vlan6
O 44.44.44.44/32 [110/3] via 10.1.5.1, 04:13:23, vlan6
O 55.55.55.55/32 [110/2] via 10.1.5.1, 04:17:36, vlan6
```

---

## Note

- Device 1, Device 2, Device 3 and Device 4 are viewed the same way as that for Device 5, and the viewing process is omitted.
- 

Step 4: Enable multicast forwarding globally, enable the multicast protocol PIM-SM on the interfaces, and configure C-BSR and C-RP.

#Configure Device 1. Enable multicast forwarding globally, and enable the multicast protocol PIM-SM on the interfaces.

```
Device1(config)#ip multicast-routing
```

```
Device1(config)#interface vlan 2
```

```
Device1(config-if-vlan2)#ip pim sparse-mode
```

```
Device1(config-if-vlan2)#exit
```

```
Device1(config)#interface vlan 3
```

```
Device1(config-if-vlan3)#ip pim sparse-mode
```

```
Device1(config-if-vlan3)#exit
```

#Configure Device 2. Enable multicast forwarding globally, enable the multicast protocol PIM-SM on the interfaces, and configure Loopback 1 as C-RP. The range of multicast groups served by C-RP is 224.0.0.0/4.

```
Device2(config)#ip multicast-routing
Device2(config)#interface loopback0
Device2(config-if-loopback0)#ip pim sparse-mode
Device2(config-if-loopback0)#exit
Device2(config)#interface loopback1
Device2(config-if-loopback1)#ip pim sparse-mode
Device2(config-if-loopback1)#exit
Device2(config)#interface vlan 3
Device2(config-if-vlan3)#ip pim sparse-mode
Device2(config-if-vlan3)#exit
Device2(config)#interface vlan 4
Device2(config-if-vlan4)#ip pim sparse-mode
Device2(config-if-vlan4)#exit
Device2(config)#ip pim rp-candidate loopback1
```

#Configure Device 3. Enable multicast forwarding globally, enable the multicast protocol PIM-SM on the interfaces, and configure Loopback 0 as C-BSR.

```
Device3(config)#ip multicast-routing
Device3(config)#interface loopback0
Device3(config-if-loopback0)#ip pim sparse-mode
Device3(config-if-loopback0)#exit
Device3(config)#interface vlan 4
Device3(config-if-vlan4)#ip pim sparse-mode
Device3(config-if-vlan4)#exit
Device3(config)#interface vlan 5
Device3(config-if-vlan5)#ip pim sparse-mode
Device3(config-if-vlan5)#exit
Device3(config)#ip pim bsr-candidate loopback0
```

#Configure Device 4. Enable multicast forwarding globally, enable the multicast protocol PIM-SM on the interfaces, and configure Loopback 1 as C-RP. The range of multicast groups served by C-RP is 224.0.0.0/4.

```
Device4(config)#ip multicast-routing
Device4(config)#interface loopback0
Device4(config-if-loopback0)#ip pim sparse-mode
```

```

Device4(config-if-loopback0)#exit
Device4(config)#interface loopback1
Device4(config-if-loopback1)#ip pim sparse-mode
Device4(config-if-loopback1)#exit
Device4(config)#interface vlan 5
Device4(config-if-vlan5)#ip pim sparse-mode
Device4(config-if-vlan5)#exit
Device4(config)#interface vlan 6
Device4(config-if-vlan6)#ip pim sparse-mode
Device4(config-if-vlan6)#exit
Device4(config)#ip pim rp-candidate loopback1

```

**#Configure Device 5. Enable multicast forwarding globally, and enable the multicast protocol PIM-SM on the interfaces.**

```

Device5(config)#ip multicast-routing
Device5(config)#interface vlan 6
Device5(config-if-vlan6)#ip pim sparse-mode
Device5(config-if-vlan6)#exit
Device5(config)#interface vlan 7
Device5(config-if-vlan7)#ip pim sparse-mode
Device5(config-if-vlan7)#exit

```

**#View, for Device 5, interface information with PIM-SM protocol enabled and PIM-SM neighbor information.**

```

Device5#show ip pim interface
PIM Interface Table:
PIM VRF Name: Default
Total 3 Interface entries
Total 0 External Interface entry
Total 0 Sparse-Dense Mode Interface entry

```

Address	Interface	VIF Index	Ver/ Mode	VIF Flag	Nbr Count	DR Pri	DR	BSR Border	CISCO Neighbor Filter	Neighbor
10.1.5.2	register_vif0	1	v2/S	UP						
10.1.5.2	vlan6	0	v2/S	UP	1 1	10.1.5.2		FALSE	FALSE	
10.1.6.1	vlan7	2	v2/S	UP	0 1	10.1.6.1		FALSE	FALSE	

```

Device5#show ip pim neighbor
PIM Neighbor Table:
PIM VRF Name: Default

```

Total 1 Neighbor entry

Neighbor Address	Interface	Uptime/Expires	Ver	DR Priority/Mode
10.1.5.1	vlan6	18:37:22/00:01:45	v2	1 /

#### #View the BSR and RP information of Device 5.

```
Device5#show ip pim bsr-router
```

PIMv2 Bootstrap information

PIM VRF Name: Default

**BSR address: 44.44.44.44**

BSR Priority: 0

Hash mask length: 10

Up time: 04:36:44

Expiry time: 00:01:35

Role: Non-candidate BSR

State: Accept Preferred

```
Device5#show ip pim rp mapping
```

PIM Group-to-RP Mappings Table:

PIM VRF Name: Default

Total 1 RP set entry

Total 1 RP entry

**Group(s): 224.0.0.0/4**

RP count: 1

**RP: 55.55.55.55**

Info source: 44.44.44.44, via bootstrap, priority 192

Up time: 04:36:44

Expiry time: 00:01:53

---

### Note

- Device 1, Device 2, Device 3 and Device 4 are viewed the same way as that for Device 5, and the viewing process is omitted.
- 

Step 5: Configure MSDP.

#Configure Device 2. Configure to establish a non-direct MSDP peer-to-peer connection with Loopback 0 of Device 4 via Loopback 0; enable the function of actively sending the SA request packet to the specified peer; configure the RP address in the SA packet as the IP address of Loopback 0; configure the use of RFC3618 rules to perform the RPF check on MSDP packets.

```
Device2(config)#ip msdp peer 22.22.22.22 connect-source loopback0
Device2(config)#ip msdp sa-request 22.22.22.22
Device2(config)#ip msdp originator-id loopback0
Device2(config)#ip msdp rpf rfc3618
```

#Configure Device 4. Configure to establish a non-direct MSDP peer-to-peer connection with Loopback 0 of Device 2 via Loopback 0; enable the function of actively sending the SA request packet to the specified peer; configure the RP address in the SA packet as the IP address of Loopback 0; configure the use of RFC3618 rules to perform the RPF check on MSDP packets.

```
Device4(config)#ip msdp peer 11.11.11.11 connect-source loopback0
Device4(config)#ip msdp sa-request 11.11.11.11
Device4(config)#ip msdp originator-id loopback0
Device4(config)#ip msdp rpf rfc3618
```

#View the MSDP peer-to-peer connection status and details of Device 4.

```
Device4#show ip msdp summary
MSDP Peer Status Summary
Total 1 Peer entry
Peer Address  AS   State  Reset  Uptime/Downtime
11.11.11.11  ?   Up     0      05:49:35

Device4#show ip msdp peer
MSDP Peer 11.11.11.11, AS ?

Connection status:
State: Established, Resets: 0, Connection source: loopback0
Uptime(Downtime): 05:49:39, Message sent/received: 352/528
Connection and counters cleared 05:53:24 ago
Local Address of connection: 22.22.22.22
Remote Address of connection: 11.11.11.11
Local Port: 639, Remote Port: 1053
SA-Requests:
Input filter: none
Sending SA-Requests to peer: enabled
SA:
```

```
Input filter: none
Message counters:
RPF Failure count: 3
SA Messages in/out: 348/0
SA Requests in/out: 0/3
SA Responses in/out: 2/0
Data Packets in/out: 0/0
```

It is indicated that Device 4 and Device 2 have successfully established the MSDP peer-to-peer connection.

---

## Note

- Device 2 is viewed the same way as Device 4, and the viewing process is omitted.
- 

Step 6: Check the result.

#Source sends the multicast service packet of the multicast group 225.1.1.1.

#View the MSDP SA cache information of Device 2.

```
Device2#show ip msdp sa-cache
MSDP Source-Active Cache - 1 entries
(10.1.1.2, 225.1.1.1), RP 55.55.55.55, Originated, 00:03:34/00:05:43
```

It is indicated that the SA packet is generated and cached on Device 2. In the SA packet, the multicast source address is 10.1.1.2, the multicast group address is 225.1.1.1, and the RP address is 55.55.55.55.

#View the MSDP SA cache information and RPF checklist of Device 4.

```
Device4#show ip msdp sa-cache
MSDP Source-Active Cache - 1 entries
(10.1.1.2, 225.1.1.1), RP 11.11.11.11, Recv From Peer 11.11.11.11, 00:07:02/00:05:58
```

```
Device4#show ip msdp rpf
Destination  Nextthop  Nextthop  Nextthop Metric Pref
Address      Address    From       RefCnt
10.1.4.1     0.0.0.0   0.0.0.0    1    10    0
```

```
11.11.11.11  10.1.4.1  55.55.55.55  3  3  110
55.55.55.55  0.0.0.0  0.0.0.0  2  1  0
```

It is indicated that Device 4 has received and cached the SA packet. This SA packet came from the peer 11.11.11.11. In the packet, the multicast source address is 10.1.1.2, the multicast group address is 225.1.1.1, and the RP address is 11.11.11.11.

---

## Note

- If **ip msdp originator-id** is configured on the source RP, it replaces the RP address in the SA packet with the IP address of the specified interface when sending the SA packet to the MSDP peer.
- 

#View the PIM-SM multicast routing table of Device 2.

```
Device2#show ip pim mroute
IP Multicast Routing Table:
PIM VRF Name: Default
Total 0 (*,*,RP) entry
Total 0 (*,G) entry
Total 1 (S,G) entry
Total 1 (S,G,rpt) entry
Total 0 FCR entry
Up timer/Expiry timer
```

```
(10.1.1.2, 225.1.1.1)
```

```
Up time: 00:01:14
KAT time: 00:03:23
RPF nbr: 10.1.2.1
RPF idx: vlan3
SPT bit: FALSE
Flags:
Upstream State: NOT JOINED
Local interface list:
Joined interface list:
Asserted interface list:
Outgoing interface list:
```

```
Packet count 0

(10.1.1.2, 225.1.1.1, rpt)
Up time: 00:01:14
RP: 55.55.55.55
Flags:
RPF SGRPT XG EQUAL
Upstream State: RPT NOT JOINED
Local interface list:
Pruned interface list:
Outgoing interface list:
```

#### #View the PIM-SM multicast routing table of Device 4.

```
Device4#show ip pim mroute
IP Multicast Routing Table:
PIM VRF Name: Default
Total 0 (*,*,RP) entry
Total 0 (*,G) entry
Total 0 (S,G) entry
Total 0 (S,G,rpt) entry
Total 0 FCR entry
Up timer/Expiry timer
```

It is indicated that there is entry (10.1.1.2, 225.1.1.1) on Device 2 and no entry (10.1.1.2, 225.1.1.1) on Device 4, indicating that Source initiates PIM-SM registration with the nearest RP, Device 2.

#Receiver sends an IGMPv2 member report packet to join the multicast group 225.1.1.1.

#### #View the multicast membership table on Device 5.

```
Device5#show ip igmp groups
IGMP Connected Group Membership
Total 1 groups
Group Address  Interface          Uptime  Expires  Last Reporter  V1 Expires  V2 Expires
225.1.1.1     vlan7                00:00:12 00:04:12 10.1.6.2       stopped
```

#### #View the PIM-SM multicast routing table of Device 2.

```
Device2#show ip pim mroute
IP Multicast Routing Table:
PIM VRF Name: Default
```

Total 0 (\*,\*,RP) entry  
Total 0 (\*,G) entry  
Total 1 (S,G) entry  
Total 1 (S,G,rpt) entry  
Total 0 FCR entry  
Up timer/Expiry timer

(10.1.1.2, 225.1.1.1)

Up time: 00:19:01  
KAT time: 00:03:14  
RPF nbr: 10.1.2.1  
RPF idx: vlan3  
SPT bit: TRUE  
Flags:  
JOIN DESIRED  
Upstream State: JOINED  
Local interface list:  
Joined interface list:  
vlan4 00:02:56/00:02:34  
Asserted interface list:  
Outgoing interface list:  
vlan4  
Packet count 1136269

(10.1.1.2, 225.1.1.1, rpt)

Up time: 00:19:01  
RP: 55.55.55.55  
Flags:  
RPF SGRPT XG EQUAL  
Upstream State: RPT NOT JOINED

#### #View the PIM-SM multicast routing table of Device 4.

Device4#show ip pim mroute  
IP Multicast Routing Table:  
PIM VRF Name: Default  
Total 0 (\*,\*,RP) entry  
Total 1 (\*,G) entry  
Total 1 (S,G) entry

Total 1 (S,G,rpt) entry  
Total 0 FCR entry  
Up timer/Expiry timer

(\*, 225.1.1.1)

Up time: 00:05:54  
RP: 55.55.55.55  
RPF nbr: 0.0.0.0  
RPF idx: None  
Flags:  
JOIN DESIRED  
Upstream State: JOINED  
Local interface list:  
Joined interface list:  
vlan6 00:05:54/00:02:36  
Asserted interface list:

(10.1.1.2, 225.1.1.1)

Up time: 00:05:54  
KAT time: 00:03:22  
RPF nbr: 10.1.4.1  
RPF idx: vlan5  
SPT bit: TRUE  
Flags:  
JOIN DESIRED  
Upstream State: JOINED  
Local interface list:  
Joined interface list:  
vlan6 00:05:54/00:02:37  
Asserted interface list:  
Outgoing interface list:  
vlan6  
Packet count 2172581

(10.1.1.2, 225.1.1.1, rpt)

Up time: 00:05:54

RP: 55.55.55.55  
Flags:  
RPT JOIN DESIRED  
PRUNE DESIRED  
RPF SGRPT XG EQUAL  
Upstream State: PRUNED  
Local interface list:  
Pruned interface list:  
Outgoing interface list:  
vlan6

It is indicated that there is entry (\*,225.1.1.1) on Device 4, and there is no entry (\*,225.1.1.1) on Device 2, indicating that Receiver initiates a PIM-SM join to the nearest RP, Device 4.

#Receiver can only receive the multicast service packet of the multicast group 225.1.1.1 sent by Source.

# 72 MLD

---

## 72.1 Overview

MLD is the abbreviation of Multicast Listener Discovery Protocol. It is used to establish and maintain multicast group membership between an IPv6 host and multicast devices directly adjacent thereto. The MLD router uses the IPv6 unicast link local address as the source address to send MLD packets.

MLD uses ICMPv6 (Internet Control Message Protocol for IPv6) packet type. All MLD packets are restricted to the local link with a hop count of 1.

There are 2 versions of MLD, MLDv1 corresponds to IGMPv2, and MLDv2 corresponds to IGMPv3. Unlike the IGMP protocol that uses the packet type of IP protocol number 2, the MLD protocol uses the ICMPv6 (IP protocol number 58) packet type, including MLD query packet (type value 130), MLDv1 report packet (type value 131), MLDv1 leave packet (type value 132) and MLDv2 report packet (type value 143). Except for the different packet formats, the MLD protocol and the IGMP protocol have exactly the same protocol behavior.

## 72.2 MLD Function Configuration

### 72.2.1 Configure Basic Functions of MLD

#### Configuration Condition

Before configuring the basic functions of MLD, do the following:

- Configure interface IPv6 enable.
- Configure interface MLD enable.

#### Enable MLD Protocol

Table 72-1 Enabling MLD Protocol

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Enable IPv6 multicast forwarding	<b>ipv6 multicast-routing</b> [ <i>vrf vrf-name</i> ]	Mandatory By default, IPv6 multicast forwarding is not enabled
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Enable MLD Protocol	<b>ipv6 mld enable</b>	Mandatory By default, MLD is not enabled.  All MLD-related configurations can only take effect after MLD is enabled

### Configure MLD Version

Table 72-2 Configuring MLD Version

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure MLD Version	<b>ipv6 mld version</b> <i>version-number</i>	Mandatory By default, the MLD version is 2

---

 **Note**

- Because the packet structures and types of different versions of MLD protocol are different, it is recommended that all devices on the same subnet be configured with the same version of MLD.
- 

### Configure static group joining

After the certain static group or source group is configured on the interface, the device considers that there are receivers of this multicast group or source group on the interface.

Table 72–3 Configuring Static Group Joining

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure static group joining	<b>ipv6 mld static-group</b> <i>group-ipv6-address</i> [ <i>source-ipv6-address</i> ]	Mandatory By default, the interface does not statically join any multicast group or source group

### Configure multicast group filter

The interface configured with the MLD multicast group filter will filter the group membership reports in that network segment according to the ACL rules. Only the group membership reports allowed by the ACL will be processed, and those that are not allowed will be dropped. For the existing multicast group that is not allowed by the ACL, the information of this multicast group will be deleted immediately.

Table 72–4 Configuring Multicast Group Filter

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure MLD multicast group filter	<b>ipv6 mld access-group</b> { <i>access-list-number</i>   <i>access-list-name</i> }	Mandatory By default, no multicast group filter is configured

---

### Note

- The command `ipv6 mld access-group` only supports extended ACL.
- 

## 72.2.2 Adjust and Optimize MLD Network

### Configuration Condition

Before adjusting and optimizing the MLD network, do the following:

- Enable the IPv6 protocol.
- Enable the MLD protocol.

### Configure Query Interval of General Group

MLD querier periodically sends the query packets of the general group to maintain the group membership. The interval of sending the MLD general group query packets can be modified according to the actuality of the network.

Table 72-5 Configure Query Interval of General Group

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure Query Interval of General Group	<b>ipv6 mld query-interval</b> <i>interval-value</i>	Optional By default, the interval of sending the MLD general group query packets is 125 seconds

---

### Note

- The value of the general query interval of the devices on the same network segment should be kept as consistent as possible.
  - The query interval of the general group should be larger than the maximum response time. Otherwise, the configuration cannot succeed
- 

### Configure robustness variable

Table 72–6 Configuring Robustness Variable

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface	<b>interface</b> <i>interface-name</i>	-

Step	Command	Description
configuration mode		
Configure robustness variable	<b>ipv6 mld robustness-variable</b> <i>variable-value</i>	Optional By default, the robustness variable of the MLD querier is 2

### Note

- After configuring the robustness variable, the following parameters will also vary as the robustness parameter varies:
  1. group member timeout = robustness variable \* general group query time + maximum response time;
  2. other querier timeout = robustness variable \* general group query time + maximum response time / 2;

### Configure Max. Response Time

The general group query packet sent by the MLDv1 querier contains the maximum response time field. The receiver sends the membership report packet within the maximum response interval. If the receiver does not send the group membership report within the maximum response time interval, the device considers that this subnet does not have a receiver for this multicast group and immediately deletes the multicast group information.

Table 72-7 Configure Maximum Response Time

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-

Step	Command	Description
Configure Max. Response Time	<b>ipv6 mld query-max-response-time</b> <i>seconds</i>	Optional By default, the maximum response time for MLD general group query is 10 seconds

### Configure specified group query

When the MLD querier receives the leave packet of the certain multicast group, it sends the specified group query packet "specified group query count" times to query this network segment for the multicast group, so as to learn whether the subnet has the members of the multicast group. If not receiving the membership report on the multicast group after waiting for "max response time", delete the information of the multicast group.

Table 72–8 Configuring Specified Group Query

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure Query Interval of Specified Group	<b>ipv6 mld last-member-query-interval</b> <i>interval-value</i>	Optional By default, the interval of sending the specified group query packets is 1 second
Configure specified group query count	<b>ipv6 mld last-member-query-count</b> <i>count-value</i>	Optional By default, the count of sending the specified

Step	Command	Description
		group query packets is 2

### Configure Fast Leave

Only one host is connected to the stub segment of the network to frequently switch the multicast groups. To reduce the leave delay, you can configure the multicast group fast leave on the device.

If the device receives the leave packet of one multicast group after configuring fast leave, the device checks whether the multicast group is within the fast leave range. If yes, the device does not send the specified group query packet within the network segment any more and the information of the multicast group is deleted at once.

Table 72-9 Configuring Fast Leave

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure the range of fast leave from the multicast group	<b>ipv6 mld immediate-leave</b> { <i>access-list-number</i>   <i>access-list-name</i> }	Mandatory By default, fast leave from the multicast group is not allowed.

## 72.2.3 Configure MLD SSM Mapping

### Configuration Condition

Before configuring IGMP SSM mapping, do the following:

- Enable IPv6

- Enable the MLD protocol.

### Configure MLD SSM Mapping

In the IPv6 PIM-SSM network, you can configure the MLD SSM mapping (MLD SSM Mapping) function on the device, in order to provide IPv6 PIM-SSM services to receivers that do not support MLDv2.

The user can configure MLD SSM mapping rules according to the needs of the network receivers. The group membership reports allowed by the rules are converted into MLD non-(IS\_EX, TO\_EX) membership reports, and the multicast source address is the source address specified by the MLD SSM mapping rules.

Table 72-10 Configuring MLD SSM Mapping

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable MLD SSM Mapping	<b>ipv6 mld ssm-map enable</b>	Mandatory By default, MLD SSM Mapping is not enabled
Configure MLD SSM Mapping rules	<b>ipv6 mld ssm-map static</b> <i>{ access-list-number   access-list-name }</i> <i>source-ipv6-address</i>	Mandatory By default, there are no MLD SSM Mapping rules

---

### Note

- The command `ipv6 mld ssm-map static` only supports extended ACL.
-

## 72.2.4 MLD Monitoring and Maintaining

Table 72-11 MLD Monitoring and Maintaining

Command	Description
<b>clear ipv6 mld group</b> [ <i>group-ipv6-address</i> ] [ <b>vrf</b> <i>vrf-name</i> ] [ <i>interface-name</i> ]	Clear MLD multicast group information
<b>clear ipv6 mld statistic interface</b> <i>interface-name</i>	Clear MLD packet statistics on the interface
<b>show ipv6 mld groups</b> [ [ <b>static</b> ]   [ <i>interface-name</i> ] [ <i>group-ipv6-address</i> ] [ <b>detail</b> ] ] [ <b>vrf</b> <i>vrf-name</i> ]	Show MLD multicast group information
<b>show ipv6 mld interface</b> [ <i>interface-name</i> ] [ <b>vrf</b> <i>vrf-name</i> ]	Show interface MLD information
<b>show ipv6 mld statistic interface</b> <i>interface-name</i> [ <b>vrf</b> <i>vrf-name</i> ]	Show statistics of MLD packets

## 72.3 MLD Typical Configuration Example

### 72.3.1 Configure Basic Functions of MLD

#### Network Requirements

- The IPv6 PIM-SM protocol runs on the entire network.
- Device 1, Device 2, and Receiver are in the same LAN, and Device 1 is the querier.
- Receiver is one receiver of the Device 1 and Device 2 stub network.
- MLDv2 runs between the Device 1 and Device 2 and the stub network.

#### Network Topology

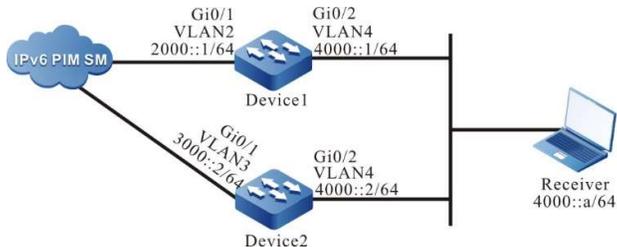


Figure 72-1 Network Topology for Configuring Basic Functions of MLD

### Configuration Steps

- Step 1: Configure VLANs, and add the port to the corresponding VLAN (omitted).
- Step 2: Configure the IPv6 address of each interface (omitted).
- Step 3: Enable IPv6 multicast forwarding globally, enable the multicast protocol IPv6 PIM-SM on each interface, and enable MLD on the interface connecting Device 1 and Device 2 to Receiver.

#### #Configure Device1.

Enable IPv6 multicast forwarding globally, enable the multicast protocol IPv6 PIM-SM on related interfaces, and enable MLD on the interface connecting to Receiver.

```
Device1#configure terminal
Device1(config)#ipv6 multicast-routing
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ipv6 pim sparse-mode
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan4
Device1(config-if-vlan4)#ipv6 pim sparse-mode
Device1(config-if-vlan4)#ipv6 mld enable
Device1(config-if-vlan4)#exit
```

#### #Configure Device2.

Enable IPv6 multicast forwarding globally, enable the multicast protocol IPv6 PIM-SM on related interfaces, and enable MLD on the interface connecting to Receiver.

```
Device2#configure terminal
Device2(config)#ipv6 multicast-routing
Device2(config)#interface vlan3
Device2(config-if-vlan3)#ipv6 pim sparse-mode
Device2(config-if-vlan3)#exit
```

```
Device2(config)#interface vlan4
Device2(config-if-vlan4)#ipv6 pim sparse-mode
Device2(config-if-vlan4)#ipv6 mld enable
Device2(config-if-vlan4)#exit
```

Step 4: Check the result.

#View the MLD version information and querier election result of Device 1 interface vlan 4.

```
Device1#show ipv6 mld interface vlan4
Interface vlan4 (Index 23)
MLD Enabled, Active
Querier: fe80::201:2ff:fe03:406 (Self)
Default version: 2
Querier parameter:
Query interval is 125 seconds
Querier timeout is 255 seconds
Query response time is 10 seconds
Last member query response interval is 1 seconds
Last member query count is 2
Group Membership interval is 260 seconds
Robustness variable is 2
```

#View the MLD version information and querier election result of Device 2 interface vlan 4.

```
Device2#show ipv6 mld interface vlan4
Interface vlan4 (Index 50331674)
MLD Enabled, Active
Querier: fe80::201:2ff:fe03:406
Non-Querier: fe80::201:7aff:febc:662b Expires: 00:04:07
Default version: 2
Querier parameter:
Query interval is 125 seconds
Querier timeout is 255 seconds
Query response time is 10 seconds
Last member query response interval is 1 seconds
Last member query count is 2
Group Membership interval is 260 seconds
Robustness variable is 2
```

#Receiver sends an MLDv2 membership report to join the multicast group FF1E::1.

#View the multicast membership table of Device 1.

```

Device1#show ipv6 mld groups
MLD Connected Group Membership
Total 1 Connected Groups
Group          Interface    Uptime    Expires V1-Expires Last Reporter
ff1e::1        vlan4        00:00:02  00:04:17 not used  fe80::b

```

#View the multicast membership table of Device 2.

```

Device2#show ipv6 mld groups
MLD Connected Group Membership
Total 1 Connected Groups
Group          Interface    Uptime    Expires V1-Expires Last Reporter
ff1e::1        vlan4        00:00:02  00:04:17 not used  fe80::b

```

---

## Note

- The interface runs the MLDv2 version by default, which is compatible with MLDv1 membership reports and MLDv1 member leave packets. By means of the command `ipv6 mld version` you can configure the version of IGMP that runs on the interface.
  - When multiple devices in the same LAN run MLD, the election of MLD queriers will be performed, and one with the smaller Link-Local address is elected as the IGMP querier of this LAN.
- 

## 72.3.2 Configure MLD Static Group Joining

### Network Requirements

- The IPv6 PIM-SM protocol runs on the entire network.
- Receiver is one receiver of Device stub network.
- MLDv2 runs between Device and the stub network.
- Interface vlan 3 of Device joins the multicast group FF1E::1 in a static way.

### Network Topology



Figure 72-2 Network Topology for Configuring MLD Static Group Joining

### Configuration Steps

- Step 1: Configure VLANs, and add the port to the corresponding VLAN (omitted).
- Step 2: Configure the IPv6 address of each interface (omitted).
- Step 3: Enable IPv6 multicast forwarding globally, enable the multicast protocol IPv6 PIM-SM on each interface, and enable MLD on the interface connecting to Receiver.

#### #Configure Device.

Enable IPv6 multicast forwarding globally, enable the multicast protocol IPv6 PIM-SM on related interfaces, and enable MLD on the interface connecting to Receiver.

```
Device#configure terminal
Device(config)#ipv6 multicast-routing
Device(config)#interface vlan2
Device(config-if-vlan2)#ipv6 pim sparse-mode
Device(config-if-vlan2)#exit
Device(config)#interface vlan3
Device(config-if-vlan3)#ipv6 pim sparse-mode
Device(config-if-vlan3)#ipv6 mld enable
Device(config-if-vlan3)#exit
```

#### #View the MLD information of the interface vlan 3 of Device.

```
Device#show ipv6 mld interface vlan3
Interface vlan3 (Index 23)
MLD Enabled, Active
Querier: fe80::201:2ff:fe03:406 (Self)
Default version: 2
Querier parameter:
  Query interval is 125 seconds
  Querier timeout is 255 seconds
  Query response time is 10 seconds
  Last member query response interval is 1 seconds
  Last member query count is 2
  Group Membership interval is 260 seconds
  Robustness variable is 2
```

- Step 4: Interface vlan 3 of Device joins the multicast group FF1E::1 in a static way.

## #Configure Device.

Configure the static multicast group FF1E::1 on the interface vlan 3 of Device.

```
Device(config)#interface vlan3
Device(config-if-vlan3)#ipv6 mld static-group ff1e::1
Device(config-if-vlan3)#exit
```

Step 5: Check the result.

#Source sends the multicast packet of the multicast group FF1E::1.

#View the multicast membership table of Device.

```
Device#show ipv6 mld groups
MLD Static Group Membership
Total 1 Static Groups
Group      Source      Interface
ff1e::1    ::          vlan3
```

#View the multicast routing table of Device.

```
Device#show ipv6 pim mroute
IP Multicast Routing Table:
PIM6 VRF Name: Default
Total 0 (*,*,RP) entry
Total 1 (*,G) entry
Total 1 (S,G) entry
Total 1 (S,G,rpt) entry
Total 0 FCR entry
Up timer/Expiry timer
```

```
(*, ff1e::1)
Up time: 00:01:06
RP: ::
RPF nbr: ::
RPF idx: None
Flags:
Upstream State: NOT JOINED
Local interface list:
    vlan3
Joined interface list:
```

Asserted interface list:

(1000::a, ff1e::1)

Up time: 00:00:04

KAT time: 00:03:26

RPF nbr: ::

RPF idx: None

SPT bit: TRUE

Flags:

JOIN DESIRED

COULD REGISTER

Upstream State: JOINED

Local interface list:

Joined interface list:

register\_vif0

Asserted interface list:

Outgoing interface list:

register\_vif0

vlan3

Packet count 1

(1000::a, ff1e::1, rpt)

Up time: 00:00:04

RP: ::

Flags:

RPT JOIN DESIRED

RPF SGRPT XG EQUAL

Upstream State: NOT PRUNED

Local interface list:

Pruned interface list:

Outgoing interface list:

#Receiver can receive multicast packets of the multicast group FF1E::1 sent by Source.

### 72.3.3 Configure MLD SSM Mapping

#### Network Requirements

- The IPv6 PIM-SSM protocol runs on the entire network.

- Receiver 1, Receiver 2, and Device 2 are in the same LAN.
- MLDv2 runs between Device 2 and the stub network.
- By using MLD SSM mapping on Device 2, Receiver 2 can only receive multicast packets sent by Source 1.

### Network Topology

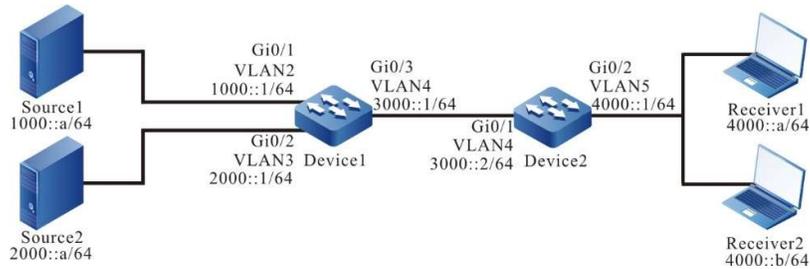


Figure 72-3 Network Topology for Configuring MLD SSM Mapping

### Configuration Steps

- Step 1: Configure VLANs, and add the port to the corresponding VLAN (omitted).
- Step 2: Configure the IPv6 address of each interface (omitted).
- Step 3: Enable IPv6 unicast routing protocol OSPFv3, so that all devices in the network can communicate with each other.

#### #Configure Device1.

```

Device1#configure terminal
Device1(config)#ipv6 router ospf 100
Device1(config-ospf6)#router-id 1.1.1.1
Device1(config-ospf6)#exit
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ipv6 router ospf 100 area 0
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan3
Device1(config-if-vlan3)#ipv6 router ospf 100 area 0
Device1(config-if-vlan3)#exit
Device1(config)#interface vlan4
Device1(config-if-vlan4)#ipv6 router ospf 100 area 0
Device1(config-if-vlan4)#exit

```

#### #Configure Device2.

```
Device2#configure terminal
Device2(config)#ipv6 router ospf 100
Device2(config-ospf6)#router-id 2.2.2.2
Device2(config-ospf6)#exit
Device2(config)#interface vlan4
Device2(config-if-vlan4)#ipv6 router ospf 100 area 0
Device2(config-if-vlan4)#exit
```

## #View the routing table of Device 2.

```
Device2#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management
```

```
L ::1/128 [0/0]
   via ::, 05:20:37, lo0
O 1000::/64 [110/2]
   via fe80::201:2ff:fe03:406, 00:35:30, vlan4
O 2000::/64 [110/2]
   via fe80::201:2ff:fe03:406, 00:37:15, vlan4
C 3000::/64 [0/0]
   via ::, 00:38:24, vlan4
L 3000::2/128 [0/0]
   via ::, 00:38:22, lo0
C 4000::/64 [0/0]
   via ::, 00:31:55, vlan5
L 4000::2/128 [0/0]
   via ::, 00:31:53, lo0
```

---

### Note

- Device 1 is viewed the same way as Device 2, and the viewing process is omitted.
-

Step 4: Enable IPv6 multicast forwarding globally, and configure IPv6 PIM-SSM globally. The range of multicast groups served by SSM is FF3X::/32. Enable the multicast protocol IPv6 PIM-SM on the interfaces. Interface vlan 5 of Device 2 runs MLDv2.

#### #Configure Device1.

Enable IPv6 multicast forwarding globally, configure IPv6 PIM-SSM globally, and enable the multicast protocol IPv6 PIM-SM on related interfaces.

```
Device1(config)#ipv6 multicast-routing
Device1(config)#ipv6 pim ssm default
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ipv6 pim sparse-mode
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan3
Device1(config-if-vlan3)#ipv6 pim sparse-mode
Device1(config-if-vlan3)#exit
Device1(config)#interface vlan4
Device1(config-if-vlan4)#ipv6 pim sparse-mode
Device1(config-if-vlan4)#exit
```

#### #Configure Device2.

Enable IPv6 multicast forwarding globally, configure IPv6 PIM-SSM globally, and enable the multicast protocol IPv6 PIM-SM on related interfaces. Interface vlan 5 runs MLDv2.

```
Device2(config)#ipv6 multicast-routing
Device2(config)#ipv6 pim ssm default
Device2(config)#interface vlan4
Device2(config-if-vlan4)#ipv6 pim sparse-mode
Device2(config-if-vlan4)#exit
Device2(config)#interface vlan5
Device2(config-if-vlan5)#ipv6 pim sparse-mode
Device2(config-if-vlan5)#ipv6 mld enable
Device2(config-if-vlan5)#exit
```

#### #View the MLD information of the interface vlan 5 of Device 2.

```
Device2#show ipv6 mld interface vlan5
Interface vlan5 (Index 23)
MLD Enabled, Active
Querier: fe80::201:2ff:fe03:406 (Self)
Default version: 2
```

Querier parameter:  
Query interval is 125 seconds  
Querier timeout is 255 seconds  
Query response time is 10 seconds  
Last member query response interval is 1 seconds  
Last member query count is 2  
Group Membership interval is 260 seconds  
Robustness variable is 2

Step 5: Enable MLD SSM mapping on Device 2 and configure MLD SSM mapping rules so that Receiver 1 and Receiver 2 can only receive multicast packets sent by Source 1.

#Configure Device2.

Enable MLD SSM mapping, and configure the range of multicast groups for MLD SSM mapping to FF3E::/64. The multicast source address is 1000::a.

```
Device2(config)#ipv6 access-list extended 7001
Device2(config-std-nacl)#permit ipv6 any ff3e::/64
Device2(config-std-nacl)#commit
Device2(config-std-nacl)#exit
Device2(config)#ipv6 mld ssm-map enable
Device2(config)#ipv6 mld ssm-map static 7001 1000::a
```

Step 6: Check the result.

#Receiver1 sends an MLDv2 membership report of the specified source group to join the multicast group FF3E::1, and the specified multicast source is 2000::a; Receiver 2 sends an MLDv1 membership report to join the multicast group FF3E::2.

#Both Source 1 and Source 2 send multicast packets of the multicast groups FF3E::1 and FF3E::2.

#View the multicast membership table of Device 2.

```
Device2#show ipv6 mld groups
MLD Connected Group Membership
Total 2 Connected Groups
Group          Interface    Uptime   Expires V1-Expires Last Reporter
ff3e::1        vlan5        00:00:33 not used not used  fe80::a
ff3e::2        vlan5        00:00:33 not used not used  fe80::b

Device2#show ipv6 mld groups detail
```

MLD Connected Group Membership

Total 2 Connected Groups

Group	Interface	Uptime	Expires	V1-Expires	Last Reporter
ff3e::1	vlan5	00:00:36	not used	not used	fe80::a

Group mode : Include

TIB-A Count: 1

TIB-B Count: 0

TIB-A

Source list: (R - Remote, M - SSM Mapping)

Source	Uptime	Expires	Flags
2000::a	00:00:36	00:03:49	R
ff3e::2	vlan5	00:00:36	not used not used fe80::b

Group mode : Include

TIB-A Count: 1

TIB-B Count: 0

TIB-A

Source list: (R - Remote, M - SSM Mapping)

Source	Uptime	Expires	Flags
1000::a	00:00:36	00:03:45	RM

**#View the multicast routing table of Device 2.**

Device2#show ipv6 pim mroute

IP Multicast Routing Table:

PIM6 VRF Name: Default

Total 0 (\*,\*,RP) entry

Total 0 (\*,G) entry

Total 2 (S,G) entries

Total 0 (S,G,rpt) entry

Total 0 FCR entry

Up timer/Expiry timer

(2000::a, ff3e::1)

Up time: 00:01:36

KAT time: 00:01:54

RPF nbr: fe80::201:2ff:fe03:406

RPF idx: vlan4

SPT bit: FALSE  
Flags:  
JOIN DESIRED  
Upstream State: JOINED  
Local interface list:  
vlan5  
Joined interface list:  
Asserted interface list:  
Outgoing interface list:  
vlan5  
Packet count 0

(1000::a, ff3e::2)  
Up time: 00:01:36  
KAT time: 00:01:54  
RPF nbr: fe80::201:2ff:fe03:406  
RPF idx: vlan4  
SPT bit: FALSE  
Flags:  
JOIN DESIRED  
Upstream State: JOINED  
Local interface list:  
vlan5  
Joined interface list:  
Asserted interface list:  
Outgoing interface list:  
vlan5  
Packet count 0

#Receiver 1 can only receive multicast packets sent by Source 2, and Receiver 2 can only receive multicast packets sent by Source 1.

---

## Note

- Device 1 is viewed the same way as Device 2, and the viewing process is omitted.
  - MLD SSM mapping needs to be used with IPv6 PIM-SSM. The range of multicast groups in the MLD SSM mapping rules must be within the range
-

---

of multicast groups of IPv6 PIM-SSM. The MLD SSM mapping provides support for the SSM model mainly for receiver hosts that run MLDv1 and cannot be upgraded to MLDv2.

- MLD SSM mapping is invalid to MLDv2 membership reports.
- 

### 72.3.4 Configure MLD Multicast Group Filtering

#### Network Requirements

- The IPv6 PIM-SM protocol runs on the entire network.
- Receiver is one receiver of Device stub network.
- MLDv2 runs between Device and the stub network.
- The interface vlan 3 of Device filters the multicast groups, and the range of multicast groups that Receiver is allowed to join is ff10::/16.

#### Network Topology



Figure 72-4 Network Topology for Configuring MLD Multicast Group Filtering

#### Configuration Steps

- Step 1: Configure VLANs, and add the port to the corresponding VLAN (omitted).
- Step 2: Configure the IPv6 address of each interface (omitted).
- Step 3: Enable IPv6 multicast forwarding globally, and enable the multicast protocol IPv6 PIM-SM on the interfaces.

#Configure Device.

Enable IPv6 multicast forwarding globally, enable the multicast protocol IPv6 PIM-SM on related interfaces, and enable MLD on the interface connecting to Receiver.

```
Device#configure terminal
Device(config)#ipv6 multicast-routing
Device(config)#interface vlan2
```

```
Device(config-if-vlan2)#ipv6 pim sparse-mode
Device(config-if-vlan2)#exit
Device(config)#interface vlan3
Device(config-if-vlan3)#ipv6 pim sparse-mode
Device(config-if-vlan3)#ipv6 mld enable
Device(config-if-vlan3)#exit
```

**#View the MLD information of the interface vlan 3 of Device.**

```
Device#show ipv6 mld interface vlan3
Interface vlan3 (Index 23)
MLD Enabled, Active
Querier: fe80::201:2ff:fe03:406 (Self)
Default version: 2
Querier parameter:
  Query interval is 125 seconds
  Querier timeout is 255 seconds
  Query response time is 10 seconds
  Last member query response interval is 1 seconds
  Last member query count is 2
  Group Membership interval is 260 seconds
  Robustness variable is 2
```

**Step 4: Configure multicast group filtering on the interface vlan 3 of Device.**

**#Configure Device.**

Configure multicast group filtering on the interface vlan3 of the Device. The range of multicast groups that Receiver is allowed to join is ff10::/16.

```
Device(config)#ipv6 access-list extended 7001
Device(config-std-nacl)#permit ipv6 any ff10::/16
Device(config-std-nacl)#commit
Device(config-std-nacl)#exit
Device(config)#interface vlan3
Device(config-if-vlan3)#ipv6 mld access-group 7001
Device(config-if-vlan3)#exit
```

**Step 5: Check the result.**

**#Receiver sends an MLDv1 membership report to join the multicast groups FF10::1 and FF11::1.**

#Source sends multicast packets of the multicast groups FF10::1 and FF11::1.

#View the multicast membership table of Device.

```
Device#show ipv6 mld groups
MLD Connected Group Membership
Total 1 Connected Groups
Group          Interface    Uptime   Expires V1-Expires Last Reporter
ff10::1        vlan3        01:06:32 00:04:15 00:04:15 fe80::b
```

#View the multicast routing table of Device.

```
Device#show ipv6 pim mroute
IP Multicast Routing Table:
PIM6 VRF Name: Default
Total 0 (*,*,RP) entry
Total 1 (*,G) entry
Total 2 (S,G) entries
Total 2 (S,G,rpt) entries
Total 0 FCR entry
Up timer/Expiry timer
```

```
(*, ff10::1)
Up time: 00:01:00
RP: ::
RPF nbr: ::
RPF idx: None
Flags:
Upstream State: NOT JOINED
Local interface list:
    vlan3
Joined interface list:
Asserted interface list:
```

```
(1000::a, ff10::1)
Up time: 00:00:06
KAT time: 00:03:24
RPF nbr: ::
RPF idx: None
SPT bit: TRUE
```

Flags:  
JOIN DESIRED  
COULD REGISTER  
Upstream State: JOINED  
Local interface list:  
vlan3  
Joined interface list:  
register\_vif0  
Asserted interface list:  
Outgoing interface list:  
register\_vif0  
vlan3  
Packet count 1

(1000::a, ff10::1, rpt)

Up time: 00:00:06

RP: ::

Flags:

RPT JOIN DESIRED  
RPF SGRPT XG EQUAL  
Upstream State: NOT PRUNED  
Local interface list:  
Pruned interface list:  
Outgoing interface list:

(1000::a, ff11::1)

Up time: 00:00:06

KAT time: 00:03:24

RPF nbr: ::

RPF idx: None

SPT bit: TRUE

Flags:

JOIN DESIRED  
COULD REGISTER  
Upstream State: JOINED  
Local interface list:  
Joined interface list:  
register\_vif0

Asserted interface list:  
Outgoing interface list:  
    register\_vif0  
Packet count 1  
  
(1000::a, ff11::1, rpt)  
Up time: 00:00:06  
RP: ::  
Flags:  
    RPF SGRPT XG EQUAL  
Upstream State: RPT NOT JOINED  
Local interface list:  
Pruned interface list:  
Outgoing interface list:

#Receiver can only receive the multicast service packet of the multicast group FF10::1 sent by Source.

---

### Note

- For filtering based on the multicast source group, you still use `ipv6 mld access-group` to implement it, and configure the corresponding source address in the associated ACL. For example, `permit ipv6 1000::/16 ff10::/16` means to permit the join of source groups having the group range within FF10::/16 and the specified source range of 1000::/16. When using this function, the interface is required to run the MLDv2 version.
-

# 73 MLD snooping

## 73.1 Overview

MLD Snooping is short for Multicast Listener Discovery Snooping. It is IPv6 multicast constraint mechanism that runs on L2 devices and is used to manage and control IPv6 multicast groups.

IGMP Snooping mainly provides the following functions:

- Listen to the MLD packets to set up multicast information. IGMP Snooping gets the downstream multicast receiver information by listening to MLD packets, realizing the forwarding of multicast service packets at the specified member port;
- Listening to MLD protocol packets. In this way, the upstream multicast router can correctly maintain the MLD membership table.

## 73.2 MLD snooping Function Configuration

Table 73-1 MLD Snooping Function Configuration List

Configuration Task	
Configure basic functions of MLD snooping	Enable MLD snooping function
	Configure MLD snooping version
	Enable MLD snooping MAC forwarding function
Configure MLD snooping querier	Enable MLD snooping querier
	Configure source IPv6 address of MLD query packet
	Configure Query Interval of General Group

Configuration Task	
	Configure Max. Response Time
	Configure Query Interval of Specified Group
	Configure Fast Leave
Configure MLD snooping router port	Configure MLD snooping router port
	Configure age time for MLD snooping dynamic router port
Configure MLD snooping TCN event	Enable fast convergence
	Configure TCN event query interval
	Configure TCN event query count

### 73.2.1 Configure basic functions of MLD snooping

In the various configuration tasks for MLD snooping, you must first enable the MLD snooping function so that the configuration of the other function features can take effect.

#### Configuration Condition

Before configuring the basic functions of MLD snooping, do the following:

- Configure VLAN.

#### Enable MLD snooping function

The MLD snooping function will run on the device only after it is enabled.

Table 73-2 Enabling MLD Snooping Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Enable the global MLD snooping function	<b>ipv6 mld snooping</b>	Mandatory  By default, the global MLD snooping function is not enabled
Enable the MLD snooping function of the specified VLAN	<b>ipv6 mld snooping vlan <i>vlan-id</i></b>	Mandatory  By default, the MLD snooping function is not enabled in the VLAN

---

### Note

- The MLD snooping function of the specified VLAN can be enabled only after the global MLD snooping function is enabled.
- 

### Configure MLD snooping version

The handling rules for the configured MLD snooping version and MLD protocol packets are as follows:

If the configured MLD snooping version is V2, the device can handle IGMP protocol packets of versions V1 and V2.

If the configured MLD snooping version is V1, the device can handle MLD protocol packets of version V1, and does not handle the protocol packets of versions V2 but floods them in the VLAN.

Table 73-3 Configuring MLD snooping Version

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Configure MLD snooping version	<b>ipv6 mld snooping</b> <b>vlan <i>vlan-id</i> version</b> <i>version-number</i>	Optional  By default, the MLD snooping version is 2

### Enable MLD snooping MAC Forwarding

Generally, MLD snooping forwards multicast service packets based on the destination MAC address in the VLAN. After configuring MLD snooping MAC forwarding, MLD snooping will forward multicast service packets based on the multicast source MAC address and multicast destination MAC address in the VLAN.

Table 73-4 MLD snooping MAC Forwarding

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable the L2 multicast MAC forwarding function in the specified VLAN	<b>ipv6 mld snooping</b> <b>vlan <i>vlan-id</i> l2-</b> <b>forwarding</b>	Mandatory  By default, the L2 multicast IP forwarding function of MLD snooping is enabled for the VLAN

### 73.2.2 Configure MLD snooping querier

If there is no L3 multicast device in the network, it cannot realize the related functions of the MLD querier. To solve the problem, you can configure the MLD snooping querier on the L2 multicast device to realize the MLD querier function. Therefore, the L2 multicast device can set up and maintain the multicast forwarding entry, so as to forward multicast service packets normally.

#### Configuration Condition

Before configuring the basic functions of MLD snooping querier, do the following:

- Enable global and intra-VLAN MLD snooping functions.

### Enable MLD snooping querier

You should first enable the MLD snooping querier function so that the configuration of the other features of the querier can take effect.

Table 73-5 Enabling IGMP snooping Querier

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable MLD snooping querier	<b>ipv6 mld snooping vlan <i>vlan-id</i> querier</b>	Mandatory  By default, the MLD snooping querier of the specified VLAN is not enabled

### Configure IPv6 Address of the Querier

The querier with IPv6 address configured takes part in the election of the MLD querier in VLAN and the querier fills the IPv6 address in the source IPv6 address field of the sent MLD group query packet.

Table 73-6 Configuring IPv6 Address of the Querier

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure IPv6 Address of the Querier	<b>ipv6 mld snooping vlan <i>vlan-id</i> querier address <i>ipv6-address</i></b>	Mandatory  By default, the querier IPv6 address of the specified VLAN is not configured



**Note**

- 
- When the querier IPv6 address is not configured, the default source IPv6 address of the querier is 0:::0, but the querier does not send the IGMP group query packet with source IP address 0.0.0.0.
- 

### Configure Query Interval of General Group

MLD querier periodically sends the query packets of the general group to maintain the group membership. You can modify the interval of sending the MLD general group query packets according to the actuality of the network. For example, if the configured general group query interval is long, it can reduce the number of the MLD protocol packets in the network, avoiding the network congestion.

Table 73-7 Configuring Query Interval of General Group

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure Query Interval of General Group	<b>ipv6 mld snooping vlan <i>vlan-id</i> querier query-interval <i>interval-value</i></b>	Optional  By default, the query interval of the general group is 125 seconds

---

### Note

- In the same VLAN, the configured query interval of the general group should be larger than the maximum response time. Otherwise, the configuration cannot succeed.
- 

### Configure Max. Response Time

The general group query packet sent by the MLD querier contains the maximum response time field. The multicast receiver sends the membership report packet within the maximum response interval. If the multicast receiver does not send the group member report packet within the maximum response time interval, the device considers that this subnet does not

have a receiver for this multicast group and immediately deletes the multicast group information.

Table 73-8 Configuring Maximum Response Time

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure Max. Response Time	<b>ipv6 mld snooping vlan <i>vlan-id</i> querier max-response-time <i>time-value</i></b>	Optional By default, the maximum response time is 10 seconds

### Note

- In the same VLAN, the configured maximum response time should be smaller than the query interval of the general group. Otherwise, the configuration cannot succeed.

### Configure Query Interval of Specified Group

When the MLD querier receives the leave packet of the certain multicast group, it sends the specified group query packet to query this segment for the multicast group, so as to learn whether the subnet has the members of the multicast group. If not receiving the member report packet of the multicast group after waiting for “max response time”, delete the information of the multicast group.

Table 73-9 Configuring Query Interval of Specified Group

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure Query Interval of Specified Group	<b>ipv6 mld snooping vlan <i>vlan-id</i> last- member-query- interval <i>interval-value</i></b>	Optional By default, the query interval of the

Step	Command	Description
		specified group is 1000 milliseconds

### Configure Fast Leave

If the device receives the leave packet of one multicast group after configuring fast leave, the device does not send the query packet of the specified group to the port any more and the information of the multicast group is deleted at once.

Table 73-10 Configuring Fast Leave

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure Fast Leave	<b>ipv6 mld snooping vlan <i>vlan-id</i> immediate-leave</b>	Mandatory  By default, the fast leave function of the specified VLAN is disabled

### Note

- There are multiple receivers of the same multicast group in the device port at the same time. When the port receives the MLD leave packet of the multicast group sent by one receiver and if fast leave is configured in the VLAN that the device port is within, the multicast services of the other receivers are interrupted.

### 73.2.3 Configure MLD snooping router port

MLD snooping router port is the port receiving MLD group query packets or multicast routing protocol packets. When the device receives the MLD member report or leave packet, it forwards the packet via MLD snooping router port. In this way, the uplink router can maintain the MLD membership table correctly.

MLD snooping router port can be dynamically learned or configured manually. MLD snooping dynamic router port refreshes the age time by regularly receiving the MLD group query packets or multicast routing protocol packets. MLD snooping static router port does not age.

### Configuration Condition

Before configuring the MLD snooping router port function, do the following:

- Enable global and intra-VLAN MLD snooping functions;
- Add port member in VLAN

### Configure IGMP snooping Static Router Port

After configuring MLD snooping static router port, the device can forward the MLD protocol packet via the port even the port does not receive the MLD group query packet or multicast routing protocol packet. It can prevent the problem that the router port ages because the services of the uplink L3 multicast device are interrupted.

Table 73-11 Configuring MLD snooping Static Router Port

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure IGMP snooping Static Router Port	<b>ipv6 mld snooping vlan <i>vlan-id</i> mrouter interface { <i>interface-name</i>   <b>link-aggregation</b> <i>link-aggregation-id</i> }</b>	Mandatory By default, the MLD snooping static router port is not configured

### Configure age time for MLD snooping dynamic router port

As long as the configured age time for the MLD snooping dynamic router port is longer, the problem can be effectively prevented that the router port ages fast because the services of the uplink L3 multicast device are interrupted.

Table 73-12 Configuring Age Time for MLD Snooping Dynamic Router Port

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Configure age time for MLD snooping dynamic router port	<b>ipv6 mld snooping vlan <i>vlan-id</i> timer router-port expiry expiry-value</b>	Optional  By default, the age time of the MLD snooping dynamic router port is 255 seconds

### 73.2.4 Configure MLD snooping TCN event

#### Configuration Condition

Before configuring the MLD snooping TCN event function, do the following:

- Enable global and intra-VLAN MLD snooping functions.

#### Enable fast convergence

When the network topology varies, a TCN event will be generated. The root port of the spanning tree will actively send a global MLD leave packet to request the MLD querier in order to send a general group query packet, achieving fast convergence.

After you enable the fast convergence of the MLD snooping TCN event, the root port of the non-spanning tree can also actively send a global MLD leave packet, achieving the fast convergence.

Table 73-13 Enabling Fast Convergence

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable fast convergence	<b>ipv6 mld snooping tcn query solicit</b>	Mandatory  By default, fast convergence is disabled in the TCN event

#### Configure TCN event query interval

When the TCN event occurs, the MLD snooping querier will send a general group query at the TCN event query interval.

Table 73-14 Configuring TCN Event Query Interval

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure TCN event query interval	<b>ipv6 mld snooping vlan <i>vlan-id</i> querier tcn query interval <i>interval-value</i></b>	Optional  By default, the TCN event query interval is 31 seconds

#### Configure TCN event query count

When the TCN event occurs, the MLD snooping querier will send a general group query at the TCN event query interval. The interval will restore to the general group query interval after the number of sending times reaches the configured TCN event query count.

Table 73-15 Configuring TCN Event Query Count

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure TCN event query count	<b>ipv6 mld snooping vlan <i>vlan-id</i> querier tcn query count <i>count-number</i></b>	Optional  By default, the TCN event query count is 2

## 73.3 Typical Configuration Example of MLD Snooping

### 73.3.1 Configure MLD snooping

#### Network Requirements

- Device 1 configures the IPv6 multicast routing protocol, Device 2 enables MLD snooping, PC 1 and PC 2 are the receivers of multicast services, and PC 3 is the receiver of non-multicast services;

- Multicast Server sends the IPv6 multicast service packets, PC 1 and PC 2 can correctly receive the multicast service packets, and PC 3 cannot receive the multicast service packets.

### Network Topology

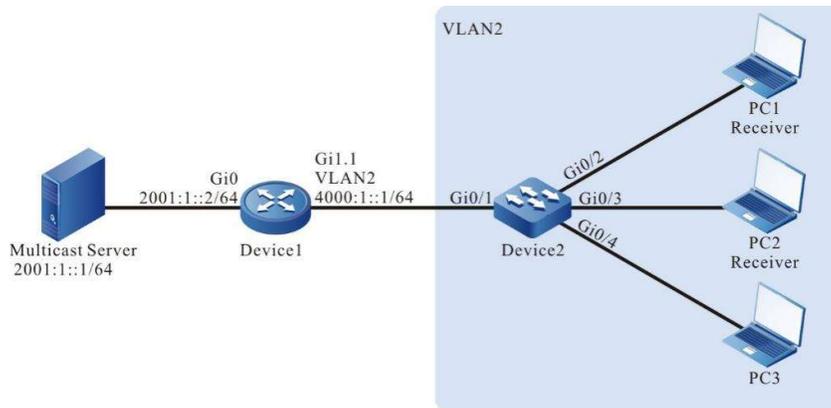


Figure 73-1 Network Topology for Configuring MLD snooping

### Configuration Steps

- Step 1: On Device 1, configure the interface IPv6 address and enable the IPv6 multicast routing protocol (omitted).
- Step 2: Configure Device2.

Create VLAN2 on #Device 2.

```
Device2#configure terminal
Device2(config)#vlan 2
Device2(config-vlan2)#exit
```

#On Device 2, configure the link type of ports gigabitethernet0/2-gigabitethernet0/4 Access to allow services of VLAN 2 to pass.

```
Device2(config)#interface gigabitethernet 0/2-0/4
Device2(config-if-range)#switchport access vlan 2
Device2(config-if-range)#exit
```

#On Device 2, configure the link type of port gigabitethernet0/1 to Trunk to allow services of VLAN 2 to pass, and configure PVID to 1.

```
Device2(config)#interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#switchport mode trunk
Device2(config-if-gigabitethernet0/1)#switchport trunk allowed vlan add 2
```

```
Device2(config-if-gigabitethernet0/1)#switchport trunk pvid vlan 1
Device2(config-if-gigabitethernet0/1)#exit
```

**#Enable unknown multicast drop in VLAN 2.**

```
Device2(config)#vlan 2
Device2(config-vlan2)#l2-multicast drop-unknown
Device2(config-vlan2)#l3-multicast ipv6 drop-unknown
Device2(config-vlan2)#exit
```

**#Enable MLD snooping and enable the routing port dynamic learning function of VLAN 2.**

```
Device2(config)#ipv6 mld snooping
Device2(config)#ipv6 mld snooping vlan 2
Device2(config)#ipv6 mld snooping vlan 2 mrouter-learning
```

**Step 3: Check the result.**

**#PC 1 and PC 2 send MLDv1 member report packets to join the IPv6 multicast group FF10::1.**

**#View the multicast membership table of Device 2.**

```
Device2#show ipv6 mld snooping groups
MLD Snooping Group Membership
Total 2 groups

VLAN ID  Port Name  Group Address  Expires  Last Reporter  V1 Expires  Uptime
-----  -
2        gi0/2     ff10::1  00:03:59  fe80::b        stopped    00:00:16
2        gi0/3     ff10::1  00:03:59  fe80::c        stopped    00:00:16
```

**#Multicast Server sends the IPv6 multicast service packet with the destination address of FF10::1, PC 1 and PC 2 can correctly receive the multicast service packet, and PC 3 cannot receive the multicast service packet.**

# 74 IPv6 Multicast Basics

## 74.1 Overview

The IPv6 multicast basics section is the basics for running the IPv6 multicast protocol and is a common part of all multicast protocols. To run any multicast routing protocol, you need to enable the IPv6 multicast forwarding function before the device can forward multicast service packets.

## 74.2 IPv6 Multicast Basics Function Configuration

Table 74-1 IPv6 Multicast Basics Function Configuration List

Configuration Task	
Enable IPv6 multicast forwarding	Enable IPv6 multicast forwarding

### 74.2.1 Enable IPv6 multicast forwarding

IPv6 multicast forwarding is the basic module of multicast forwarding. You must enable the IPv6 multicast forwarding function on the device to forward IPv6 multicast service packets. Both general IPv6 multicast forwarding and IPv6 multicast fast forwarding are to be controlled by whether IPv6 multicast forwarding is enabled.

IPv6 multicast fast forwarding refers to the design of an IPv6 fast multicast forwarding technology in order to improve the forwarding performance for service data packets. Its core is to move down the routing and service processing process, and complete routing and service processing at one time, thereby greatly reducing resource consumption caused by such as internal task switching and packet cache management in the system, and ultimately improving the data forwarding performance of the entire system.

#### Configuration Condition

Before configuring the IPv6 multicast forwarding function, do the following:

- Configure the IPv6 address of the interface so that neighbor nodes are reachable at the network layer;
- Configure any unicast routing protocol to achieve reachable routes

within the domain;

- Configure any multicast routing protocol.

### Enable IPv6 Multicast Forwarding

You must enable the IPv6 multicast forwarding function on the device to forward IPv6 multicast service packets.

Table 74-2 Enabling IPv6 Multicast Forwarding

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable IPv6 multicast forwarding	<b>ipv6 multicast-routing [ vrf vrf-name ]</b>	Mandatory Enable IPv6 multicast forwarding. By default, IPv6 multicast forwarding is not enabled

## 74.2.2 Configure IPV6 Multicast Forwarding Rules

### Configuration Condition

Before configuring the IPV6 multicast forwarding rules, do the following:

- Configure the IPV6 address of the interface so that neighbor nodes are reachable at the network layer;
- Configure any IPV6 unicast routing protocol to achieve reachable routes within the domain;
- Enable IPV6 multicast forwarding;
- Configure any IPV6 multicast routing protocol.

### Configure IPV6 Multicast Routing Table Limit

Configure the limit on the maximum number of entries in the IPV6 multicast routing table. After the maximum number of entries in the IPV6 multicast routing table exceeds the limit, no new IPV6 multicast routing table will be created.

Table 74-3 Configuring IPv6 Multicast Routing Table Limit

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure multicast routing table limit	<b>ipv6 multicast route-limit</b> <i>number-value [ vrf vrf-name ]</i>	Optional  By default, the maximum number of entries in the multicast routing table is 4096

### 74.2.3 Monitoring and Maintaining of IPv6 Multicast Basics

Table 74-4 Monitoring and Maintaining of IPv6 Multicast Basics

Command	Description
<b>clear ipv6 mcache</b> [ <i>source source-ipv6-address</i> ] [ <b>group</b> <i>group-ipv6-address</i> ] [ <b>vrf</b> <i>vrf-name</i> ]   [ <b>all</b> ]	Clear the multicast core routing table
<b>show ipv6 mcache</b> [ <b>source</b> <i>source-ipv6-address</i> ] [ <b>group</b> <i>group-ipv6-address</i> ] [ <b>vrf</b> <i>vrf-name</i> ]	Show multicast core routing table information
<b>show ipv6 mvif</b> [ <b>vrf</b> <i>vrf-name</i> ]	Show multicast virtual interface information

# 75 IPv6 PIM-SM

## 75.1 Overview

The IPv6 PIM protocol is basically the same as the IPv4 PIM protocol in behavior except for the IP address structure in the packet.

See the overview.

## 75.2 IPv6 PIM-SM Function Configuration

Table 75-1 IPv6 PIM-SM Function Configuration List

Configuration Task	
Configure basic functions of IPv6 PIM-SM	Enable IPv6 PIM-SM protocol
Configure IPv6 PIM-SM Aggregation Router	Configure C-RP
	Configure static RP
Configure IPv6 PIM-SM bootstrap router	Configure C-BSR
	Configure BSR Border
Configure IPv6 PIM-SM multicast source registration	Configure RP reachability check
	Configure sending rate of register packets

Configuration Task	
	Configure sending rate of register-stop packets
	Configure source address of register packets
	Configure register packet filtering
Configure IPv6 PIM-SM neighbor parameters	Configure sending period of HELLO packets
	Configure keepalive time of neighbors
	Configure neighbor filtering
	Configure DR priority
Configure IPv6 PIM-SM SPT switching	Configure SPT switching conditions
Configure IPv6 PIM-SSM	Configure IPv6 PIM-SSM

### 75.2.1 Configure basic functions of IPv6 PIM-SM

#### Configuration Condition

Before configuring IPv6 PIM-SM, do the following:

- Configure the network layer address of the interface so that all neighbor nodes are reachable at the network layer.
- Configure any unicast routing protocol to achieve reachable routes within the domain.

#### Enable IPv6 PIM-SM protocol

Table 75–2 Enabling IPv6 PIM-SM Protocol

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable IPv6 multicast forwarding	<b>ipv6 multicast-routing</b>	Mandatory By default, IPv6 multicast forwarding is not enabled
Enter the interface configuration mode	<b>interface <i>interface-name</i></b>	-
Enable IPv6 PIM-SM protocol	<b>ipv6 pim sparse-mode</b>	Either-or
	<b>ipv6 pim sparse-mode passive</b>	By default, the interface is in IPv6 PIM-SM shut-down status

---

### Note

- All IPv6 PIM-SM related configurations can only take effect after the IPv6 PIM-SM function is enabled.
- 

## 75.2.2 Configure IPv6 PIM-SM Aggregation Router

### Configuration Condition

Before configuring RP, do the following:

- Configure the network layer address of the interface so that all neighbor nodes are reachable at the network layer.
- Configure any unicast routing protocol to achieve reachable routes within the domain.
- Enable the IPv6 PIM-SM protocol.

## Configure C-RP

RP results from C-RP election. After BSR election, all C-RPs (Candidate-Rendezvous Point, candidate aggregation routers) regularly unicast C-RP packets to BSR. BSR integrates the C-RP information and conveys the information to all the devices within the SM domain via bootstrap packets.

Table 753 Configuring C-RP

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure C-RP	<b>ipv6 pim rp-candidate interface-name</b> [ [ <i>priority-value</i> [ <i>interval-value</i> [ <b>group-list</b> { <i>access-list-number</i>   <i>access-list-name</i> } ] ] ]   [ <b>group-list</b> { <i>access-list-number</i>   <i>access-list-name</i> } ] ] [ <b>vrf</b> <i>vrf-name</i> ]	Mandatory  By default, there are no C-RPs

---

### Note

- RP election is performed based on the following rules:
    1. the longest mask matching is performed on the range of groups served by C-RP services;
    2. compare the C-RP priorities if there are multiple C-RPs in the longest mask matching, the smaller the value, the higher the priority, and those with the higher priority win;
    3. calculate the HASH value for the C-RP addresses and groups if there is more than one C-RP with the highest priority, the C-RP with the largest HASH value wins;
    4. if there is more than one RP with the largest HASH value, the C-RP with the largest IPv6 address wins.
- 

## Configure static RP

For simple IPv6 PIM-SM networks, the static RP is recommended. The use of the static RP eliminates the need for BSR configuration and eliminates frequent interaction between RPs and BSRs, thereby saving network bandwidth.

Table 75-4 Configuring Static RP

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure static RP	<b>ipv6 pim rp-address</b> <i>ipv6-address</i> [ <i>access-list-name</i>   <i>access-list-number</i> ] [ <b>override</b> ] [ <b>vrf</b> <i>vrf-name</i> ]	Mandatory By default, there are no static RPs

### Note

- All devices in the same IPv6 PIM-SM domain must be configured with the same static RP to work normally.

## 75.2.3 Configure IPv6 PIM-SM bootstrap router

### Configuration Condition

Before configuring BSR, do the following:

- Configure the network layer address of the interface so that all neighbor nodes are reachable at the network layer.
- Configure any unicast routing protocol to achieve reachable routes within the domain.
- Enable the IPv6 PIM-SM protocol.

### Configure C-BSR

In one IPv6 PIM-SM domain, there must be unique BSR. Multiple C-BSRs (Candidate-Bootstrap Routers) result in the only recognized BSR via bootstrap packet election.

Table 75-5 Configuring C-BSR

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure C-BSR	<b>ipv6 pim bsr-candidate</b> <i>interface_name</i> [ <i>hash-mask-length</i> [ <i>priority-value</i> ] ] [ <b>vrf</b> <i>vrf-name</i> ]	Mandatory By default, there are no C-BSRs

## Note

- BSR election is performed based on the following rules:
  1. compare the priorities, the larger the value, the higher the priority, and those with the higher priority win;
  2. in the case of the same priority, those with the larger IPv6 address win.

### Configure BSR Border

BSR is responsible for collecting C-RP information and conveying this information to all devices in the IPv6 PIM-SM domain via bootstrap packets. The range of BSR is also the range of the multicast domain. Bootstrap packets cannot pass through the interfaces configured with BSR border. The devices outside the multicast domain cannot forward multicast service packets within the multicast domain. In this way, the multicast domain is divided.

Table 75-6 Configuring BSR Border

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-

Step	Command	Description
Configure BSR Border	<b>ipv6 pim bsr-border</b>	Mandatory By default, there are no multicast borders

## 75.2.4 Configure IPv6 PIM-SM multicast source registration

### Configuration Condition

Before configuring multicast source registration, do the following:

- Configure the network layer address of the interface so that all neighbor nodes are reachable at the network layer.
- Configure any unicast routing protocol to achieve reachable routes within the domain.
- Enable the IPv6 PIM-SM protocol.

### Configure RP reachability check

Before the source DR sends the register packet to RP, you may run the reachability check on RP. If RP routing is found to be unreachable, skip registering with RP, thereby reducing the overhead of this DR.

Table 75-7 Configuring RP Reachability Check

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure RP reachability check	<b>ipv6 pim register-rp-reachability</b>	Mandatory By default, RP reachability is not checked before the registration process of PIM

---

## Note

- To reduce the overhead of the source DR, it is recommended to configure this command on all source DRs of IPv6 PIM-SM.
- 

### Configure sending rate of register packets

When the source DR receives a multicast data packet, it encapsulates the multicast data packet into a register message and sends it to RP for source registration until the registration is completed.

When the source DR has not completed the registration of the multicast source and the multicast traffic is large, a large number of register packets will be generated, which will increase the burden on the RP device, and even may cause RP not to work normally. Because it is not necessary for the source DR to send all the register packets of the same flow to RP, configuring the sending rate of the register packets at the source DR can meet the purpose of source registration and reduce the burden on RP.

Table 75-8 Configuring Sending Rate of Register Packets

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure sending rate of register packets	<b>ipv6 pim register-rate-limit</b> <i>rate-limit-value</i> [ <b>vrf</b> <i>vrf-name</i> ]	Mandatory By default, the sending rate of register packets is not limited

---

## Note

- To reduce the burden on RP, it is recommended to configure the source registration sending rate on all source DRs.
- 

### Configure sending rate of register-stop packets

After RP receives a register packet from the source DR, it will send a register-stop packet to the source DR to complete the registration process. When RP receives many register packets, it is necessary to reply to all the register packets(that is, to send register-stop packets). In actual situations, there are many duplicate packets in these register-stop packets. The sending rate of the register-stop packets on RP can be limited to achieve the purpose of reducing the overhead on RP.

Table 75-9 Configuring Sending Rate of Register-stop Packets

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure sending rate of register-stop packets	<b>ipv6 pim register-stop-rate-limit</b> <i>rate-limit-value</i> [ <b>vrf</b> <i>vrf-name</i> ]	Mandatory  By default, the sending rate of register-stop packets is not limited

### Note

- To improve the robustness of the entire IPv6 PIM-SM network, it is recommended to limit the rate of source register-stop packets in all RPs.

### Configure source address of register packets

When the source DR performs source registration, the source address of the register packet uses the register interface IPv6 address automatically generated by the system. This command can specify the source address of the register packet as the IPv6 address of one interface on this device to satisfy some special needs of the network.

Table 75-10 Configuring Source Address of Register Packets

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Configure source address of register packets	<b>ipv6 pim register-source interface</b> <i>interface-name</i> [ <b>vrf</b> <i>vrf-name</i> ]	Mandatory  By default, the IPv6 address of the register interface automatically generated by the system is used as the source address of the register packet

### Configure register packet filtering

To prevent source registration attacks, ACL can be used on RP to filter the multicast source for the register packets. Only the multicast sources allowed by the ACL can successfully register with RP.

Table 75-11 Configuring Register Packet Filtering

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure register packet filtering	<b>ipv6 pim accept-register list</b> { <i>access-list-number</i>   <i>access-list-name</i> }[ <b>vrf</b> <i>vrf-name</i> ]	Mandatory  By default, register packets are not filtered

## 75.2.5 Configure IPv6 PIM-SM neighbor parameters

### Configuration Condition

Before configuring IPv6 PIM-SM neighbor parameters, do the following:

- Configure the network layer address of the interface so that all neighbor nodes are reachable at the network layer.
- Configure any unicast routing protocol to achieve reachable routes within the domain.
- Enable the IPv6 PIM-SM protocol.

### Configure sending period of HELLO packets

The interface with the IPv6 PIM-SM protocol enabled will periodically send the Hello packet to establish and maintain PIM neighbors.

Table 75-12 Configuring Sending Period of HELLO Packets

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure sending period of HELLO packets	<b>ipv6 pim hello-interval</b> <i>interval-value</i>	Optional By default, the interval of sending the Hello packet is 30 seconds

### Configure keepalive time of neighbors

When the Hello packet from one neighbor is received on the interface, the holdtime carried in the Hello packet will be recorded as the keepalive time of this neighbor. If no Hello packet of the neighbor is received within the keepalive period, this neighbor is considered invalid.

Table 75-13 Configuring IPv6 PIM-DM Neighbor Keepalive Time

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure keepalive time of neighbors	<b>ipv6 pim hello-holdtime</b> <i>holdtime-value</i>	Optional By default, the keepalive time of the IPv6 PIM-DM neighbors is 105 seconds

## Configure neighbor filtering

If there are many PIM neighbors in one subnet, you can use the neighbor filtering function to selectively establish the neighbor, thereby saving device resources.

Table 75-14 Configuring Neighbor Filtering

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure neighbor filtering	<b>ipv6 pim neighbor-filter</b> { <i>access-list-number</i>   <i>access-list-name</i> }	Mandatory By default, the neighbor filtering function is not enabled

## Configure DR priority

DR plays a very important role in the IPv6 PIM-SM network, so it is very important to select the appropriate DR. You can select the appropriate device as DR by configuring the DR priority.

Only one DR is allowed in one IPv6 PIM-SM subnet, which can be divided into source DR and sink DR according to functionality.

The main function of the source DR is to register the source with RP.

The main function of the receiving DR is to join RP and establish a switch between RPT and SPT.

Table 75-15 Configuring DR Priority

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-

Step	Command	Description
Configure DR priority	<b>ipv6 pim dr-priority</b> <i>priority-value</i>	Optional By default, the DR priority is 1

---

## Note

- DR election is performed based on the following rules:
    1. compare the priorities, the larger the value, the higher the priority, and those with the higher priority win;
    2. in the case of the same priority, those with the larger IPv6 address win.
- 

## 75.2.6 Configure IPv6 PIM-SM SPT switching

### Configuration Condition

Before configuring SPT, do the following:

- Configure the network layer address of the interface so that all neighbor nodes are reachable at the network layer.
- Configure any unicast routing protocol to achieve reachable routes within the domain.
- Enable the IPv6 PIM-SM protocol.

### Configure SPT switching conditions

The receiving DR does not know the address of the multicast source, so it can only join RP to form RPT. The source DR will register the source with RP to form the active tree between the source DR and RP. At the beginning, the direction of the multicast stream is from the multicast source to RP, and then from RP to the receiver. When the receiving DR receives the first multicast data packet, it joins the multicast source to form SPT and prunes RPT. This process is called SPT switching.

This command functions to configure SPT switching conditions at the receiving DR.

Table 75-16 Configuring SPT Switching Conditions

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure SPT switching conditions	<b>ipv6 pim spt-threshold infinity</b> [ <b>group-list</b> { <i>access-list-number</i>   <i>access-list-name</i> } ] [ <b>vrf</b> <i>vrf-name</i> ]	Mandatory By default, all multicast groups undergo SPT switching

---

## Caution

- You must not configure SPT on RP to never switch; otherwise, this will cause multicast forwarding to fail.
- 

### 75.2.7 Configure IPv6 PIM-SSM

IPv6 PIM-SSM is a subset of IPv6 PIM-SM. In IPv6 PIM-SSM, there is no need for RP, BSR, or RPT, and there is no SPT switching. Instead, the receiving DR directly joins the multicast source and establishes the shortest path tree (SPT) rooted on the source.

#### Configuration Condition

Before configuring IPv6 PIM-SSM, do the following:

- Configure the network layer address of the interface so that all neighbor nodes are reachable at the network layer.
- Configure any unicast routing protocol to achieve reachable routes within the domain.
- Enable the IPv6 PIM-SM protocol on all interfaces on which multicast routing forwarding is to be carried.

#### Configure IPv6 PIM-SSM

Table 75-17 Configuring IPv6 PIM-SSM

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure IPv6 PIM-SSM	<b>ipv6 pim ssm</b> { <b>default</b>   <b>range</b> { <i>access-list-number</i>   <i>access-list-name</i> } } [ <b>vrf</b> <i>vrf-name</i> ]	Mandatory By default, the SSM function is not enabled

## Caution

- When using IPv6 PIM-SSM, ensure that MLDv2 is enabled on the receiving DR;
- In the case that the receiver cannot upgrade to MLDv2, you can use the MLD SSM Mapping function with IPv6 PIM-SSM;

Ensure that the SSM multicast group address ranges configured on all devices in the domain are consistent, otherwise IPv6 PIM-SSM may be abnormal.

## 75.2.8 Monitoring and Maintaining of IPv6 PIM-SM

Table 75-18 Monitoring and Maintaining of IPv6 PIM-SM

Command	Description
<b>clear ipv6 pim bsr rp-set</b> [ <b>vrf</b> <i>vrf-name</i> ]	Clear RP set information of IPv6 PIM-SM
<b>clear ipv6 pim mroute</b> [ <i>group-address</i> [ <i>source-address</i> ] ] [ <b>vrf</b> <i>vrf-name</i> ]	Clear multicast routing information of IPv6 PIM-SM
<b>clear ipv6 pim statistics</b> [ [ <b>interface</b> <i>interface-name</i>   [ <b>vrf</b> <i>vrf-name</i> ] ]	Clear statistics of IPv6 PIM-SM protocol packets
<b>show ipv6 pim bsr-router</b> [ <b>vrf</b> <i>vrf-name</i> ]	Show IPv6 PIM-SM bootstrap router information

Command	Description
<b>show ipv6 pim interface</b> [ detail ]	Show IPv6 PIM-SM interface information
<b>show ipv6 pim local-members</b> <i>interface-name</i> [ vrf vrf-name ]	Show IPv6 PIM-SM local member information
<b>show ipv6 pim mroute</b> [   ssm   group <i>group-address</i> [ source <i>source-address</i> ]   source <i>source-address</i> ] [ vrf vrf-name ]	Show IPv6 PIM-SM multicast routing table information
<b>show ipv6 pim neighbor</b> [ detail ] [ vrf <i>vrf-name</i> ]	Show IPv6 PIM-SM neighbor information
<b>show ipv6 pim nexthop</b> [ <i>ipv6-address</i> ] [ vrf vrf-name ]	Show IPv6 PIM-SM next hop router information
<b>show ipv6 pim rp mapping</b> [ vrf <i>vrf-name</i> ]	Show IPv6 PIM-SM RP information
<b>show ipv6 pim rp-hash</b> <i>group-address</i> [ vrf vrf-name ]	Show RP information for IPv6 multicast group mapping
<b>show ipv6 pim statistics</b>	Show statistics of IPv6 PIM-SM protocol packets

## 75.3 Typical Configuration Example of IPv6 PIM-SM

### 75.3.1 Configure basic functions of IPv6 PIM-SM

#### Network Requirements

- The IPv6 PIM-SM protocol runs on the entire network.
- PC 1 and PC 2 are two receivers of the Device 3 stub network.
- Device 1 and Device 2 are C-BSR and C-RP.
- MLDv2 runs between Device 3 and the stub network.

#### Network Topology

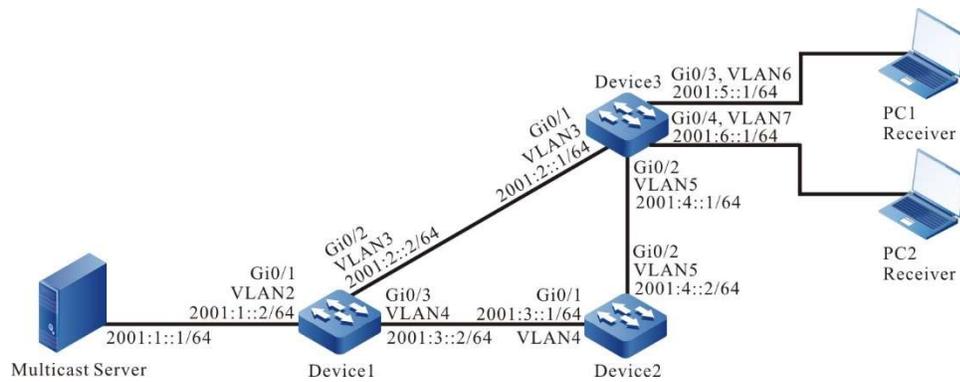


Figure 75-1 Network Topology for Configuring Basic Functions of IPv6 PIM-SM

### Configuration Steps

- Step 1: Configure VLANs, and add the port to the corresponding VLAN (omitted).
- Step 2: Configure the IPv6 address of each interface (omitted).
- Step 3: Enable the unicast routing protocol OSPFv3, so that all devices in the network can communicate with each other.

#### #Configure Device1.

```

Device1#configure terminal
Device1(config)#ipv6 router ospf 100
Device1(config-ospf6)#router-id 1.1.1.1
Device1(config-ospf6)#exit
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ipv6 router ospf 100 area 0
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan3
Device1(config-if-vlan3)#ipv6 router ospf 100 area 0
Device1(config-if-vlan3)#exit
Device1(config)#interface vlan4
Device1(config-if-vlan4)#ipv6 router ospf 100 area 0
Device1(config-if-vlan4)#exit

```

#### #Configure Device2.

```

Device2#configure terminal
Device2(config)#ipv6 router ospf 100
Device2(config-ospf6)#router-id 2.2.2.2
Device2(config-ospf6)#exit
Device2(config)#interface vlan4

```

```
Device2(config-if-vlan4)#ipv6 router ospf 100 area 0
Device2(config-if-vlan4)#exit
Device2(config)#interface vlan5
Device2(config-if-vlan5)#ipv6 router ospf 100 area 0
Device2(config-if-vlan5)#exit
```

### #Configure Device3.

```
Device3#configure terminal
Device3(config)#ipv6 router ospf 100
Device3(config-ospf6)#router-id 3.3.3.3
Device3(config-ospf6)#exit
Device3(config)#interface vlan3
Device3(config-if-vlan3)#ipv6 router ospf 100 area 0
Device3(config-if-vlan3)#exit
Device3(config)#interface vlan5
Device3(config-if-vlan5)#ipv6 router ospf 100 area 0
Device3(config-if-vlan5)#exit
Device3(config)#interface vlan6
Device3(config-if-vlan6)#ipv6 router ospf 100 area 0
Device3(config-if-vlan6)#exit
Device3(config)#interface vlan7
Device3(config-if-vlan7)#ipv6 router ospf 100 area 0
Device3(config-if-vlan7)#exit
```

### #Check the routing table of Device3.

```
Device3#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management
```

```
L ::1/128 [0/0]
   via ::, 2w6d:04:39:46, lo0
O 2001:1::/64 [110/2]
   via fe80::201:7aff:fe62:bb7e, 00:00:24, vlan3
C 2001:2::/64 [0/0]
   via ::, 00:01:05, vlan3
L 2001:2::1/128 [0/0]
   via ::, 00:01:04, lo0
O 2001:3::/64 [110/2]
   via fe80::201:7aff:fe62:bb7e, 00:00:24, vlan3
```

```
[110/2]
via fe80::201:7aff:fec0:525a, 00:00:04, vlan5
C 2001:4::/64 [0/0]
via ::, 00:00:49, vlan5
L 2001:4::1/128 [0/0]
via ::, 00:00:48, lo0
C 2001:5::/64 [0/0]
via ::, 00:00:43, vlan6
L 2001:5::1/128 [0/0]
via ::, 00:00:42, lo0
C 2001:6::/64 [0/0]
via ::, 00:00:43, vlan7
L 2001:6::1/128 [0/0]
via ::, 00:00:42, lo0
```

---

## Note

- Device1 and Device2 are checked in the same way as Device3, the process of which is omitted.
- 

Step 4: Enable IPv6 multicast forwarding globally, and enable the multicast protocol IPv6 PIM-SM on the interfaces.

### #Configure Device1.

Enable IPv6 multicast forwarding globally, and enable the multicast protocol IPv6 PIM-SM on related interfaces.

```
Device1(config)#ipv6 multicast-routing
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ipv6 pim sparse-mode
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan3
Device1(config-if-vlan3)#ipv6 pim sparse-mode
Device1(config-if-vlan3)#exit
Device1(config)#interface vlan4
Device1(config-if-vlan4)#ipv6 pim sparse-mode
Device1(config-if-vlan4)#exit
```

### #Configure Device2.

Enable IPv6 multicast forwarding globally, and enable the multicast protocol IPv6 PIM-SM on related interfaces.

```
Device2(config)#ipv6 multicast-routing
Device2(config)#interface vlan4
Device2(config-if-vlan4)#ipv6 pim sparse-mode
Device2(config-if-vlan4)#exit
Device2(config)#interface vlan5
Device2(config-if-vlan5)#ipv6 pim sparse-mode
Device2(config-if-vlan5)#exit
```

### #Configure Device3.

Enable IPv6 multicast forwarding globally, and enable the multicast protocol IPv6 PIM-SM on related interfaces.

```
Device3(config)#ipv6 multicast-routing
Device3(config)#interface vlan3
Device3(config-if-vlan3)#ipv6 pim sparse-mode
Device3(config-if-vlan3)#exit
Device3(config)#interface vlan5
Device3(config-if-vlan5)#ipv6 pim sparse-mode
Device3(config-if-vlan5)#exit
Device3(config)#interface vlan6
Device3(config-if-vlan6)#ipv6 pim sparse-mode
Device3(config-if-vlan6)#exit
Device3(config)#interface vlan7
Device3(config-if-vlan7)#ipv6 pim sparse-mode
Device3(config-if-vlan7)#exit
```

#View, for Device 3, interface information with IPv6 PIM-SM protocol enabled and IPv6 PIM-SM neighbor information.

```
Device3#show ipv6 pim interface
PIM6 Interface Table:
PIM6 VRF Name: Default
Total 5 Interface entries
Total 0 External Interface entry
Total 0 Sparse-Dense Mode Interface entry

Interface   VIF  Ver/  VIF  Nbr  DR  BSR  CISCO  Neighbor
           Index Mode  Flag Count Pri  Border Neighbor Filter
register_vif0  2    v2/S  UP
Address : fe80::201:7aff:fe5e:6d2d  Global Address: ::
```

```

vlan3      1   v2/S UP 1 1  FALSE FALSE
Address : fe80::201:7aff:fe5e:6d2d Global Address: 2001:2::1   DR: fe80::201:7aff:fe62:bb7e

vlan5      3   v2/S UP 1 1  FALSE FALSE
Address : fe80::201:7aff:fe5e:6d2e Global Address: 2001:4::1   DR: fe80::201:7aff:fec0:525a

vlan6      4   v2/S UP 0 1  FALSE FALSE
Address : fe80::201:7aff:fe5e:6d2f Global Address: 2001:5::1   DR: fe80::201:7aff:fe5e:6d2f

vlan7      5   v2/S UP 0 1  FALSE FALSE
Address : fe80::201:7aff:fe5e:6d30 Global Address: 2001:6::1   DR: fe80::201:7aff:fe5e:6d30

```

Device3#show ipv6 pim neighbor

PIM6 Neighbor Table:

PIM6 VRF Name: Default

Total 2 Neighbor entries

Neighbor Address	Interface	Uptime/Expires	Ver	DR
fe80::201:7aff:fe62:bb7e	vlan3	00:04:01/00:01:29	v2	1 / DR
fe80::201:7aff:fec0:525a	vlan5	00:04:03/00:01:39	v2	1 / DR

---

## Note

- Device1 and Device2 are checked in the same way as Device3, the process of which is omitted.
- 

Step 5: Enable MLD on vlan 6 and vlan 7 of Device 3.

#Configure Device3.

Enable MLD on vlan 6 and vlan 7 of Device 3.

```

Device3(config)#interface vlan6
Device3(config-if-vlan6)#ipv6 mld enable
Device3(config-if-vlan6)#exit
Device3(config)#interface vlan7
Device3(config-if-vlan7)#ipv6 mld enable
Device3(config-if-vlan7)#exit

```

#View the MLD information of the interfaces vlan 5 and vlan 7 of Device 3.

```
Device3#show ipv6 mld interface
Interface vlan6 (Index 11)
MLD Enabled, Active
Querier: fe80::201:7aff:fe5e:6d2f (Self)
Default version: 2
Querier parameter:
  Query interval is 125 seconds
  Querier timeout is 255 seconds
  Query response time is 10 seconds
  Last member query response interval is 1 seconds
  Last member query count is 2
  Group Membership interval is 260 seconds
  Robustness variable is 2
Interface vlan7 (Index 12)
MLD Enabled, Active
Querier: fe80::201:7aff:fe5e:6d30 (Self)
Default version: 2
Querier parameter:
  Query interval is 125 seconds
  Querier timeout is 255 seconds
  Query response time is 10 seconds
  Last member query response interval is 1 seconds
  Last member query count is 2
  Group Membership interval is 260 seconds
  Robustness variable is 2
```

---

### Note

- By means of the command `ip v6 mld version` you can configure the version of IGMP that runs on the interface.
- 

Step 6: Configure the interface vlan 3 of Device 1 as C-BSR and C-RP, and configure the interface vlan 4 of Device 2 as C-BSR and C-RP.

#Configure Device1.

Configure the interface vlan 3 of Device 1 as C-BSR and C-RP. The priority of C-BSR is 200, and the range of multicast groups served by C-RP is FF10::/16.

```
Device1(config)#ipv6 pim bsr-candidate vlan3 10 200
Device1(config)#ipv6 access-list extended 7001
Device1(config-v6-list)#permit ipv6 any ff10::/16
Device1(config-v6-list)#commit
Device1(config-v6-list)#exit
Device1(config)#ipv6 pim rp-candidate vlan3 group-list 7001
```

#Configure Device2.

Configure vlan 4 of Device 2 as C-BSR and C-RP. The priority of C-BSR is 0, and the range of multicast groups served by C-RP of Device 2 is FF00::/8.

```
Device2(config)#ipv6 pim bsr-candidate vlan4
Device2(config)#ipv6 pim rp-candidate vlan4
```

#View the BSR and RP information of Device 3

```
Device3#show ipv6 pim bsr-router
PIM6v2 Bootstrap information
PIM6 VRF Name: Default
  BSR address: 2001:2::2
  BSR Priority: 200
  Hash mask length: 10
  Up time: 00:03:04
  Expiry time: 00:02:06
  Role: Non-candidate BSR
  State: Accept Preferred
Device3#show ipv6 pim rp mapping
PIM6 Group-to-RP Mappings Table:
PIM6 VRF Name: Default
Total 2 RP set entries
Total 2 RP entries

  Group(s): ff00::/8
  RP count: 1
    RP: 2001:3::1
    Info source: 2001:2::2, via bootstrap, priority 192
    Up time: 00:21:30
    Expiry time: 00:02:24

  Group(s): ff10::/16
  RP count: 1
```

RP: 2001:2::2  
Info source: 2001:2::2, via bootstrap, priority 192  
Up time: 00:04:31  
Expiry time: 00:02:24

---

## Note

- Device 1 and Device 2 are viewed the same way as Device 3, and the viewing process is omitted;
  - When multiple C-BSRs are configured in one multicast domain, BSR will be elected according to the priority first, and C-BSR with the highest priority will be elected as BSR. When the priorities of the C-BSRs are the same, the C-BSR with the largest ip address is elected as BSR;
  - When multiple C-RPs are configured in one multicast domain and the ranges of multicast groups served are the same, RP corresponding to the multicast group G will be calculated according to the hash algorithm;
  - In the multicast domain, you can also configure RP with the command `ipv6 pim rp-address`, but the static RP addresses configured on all devices in the entire multicast domain must be consistent.
- 

Step 7: Check the result.

#PC 1 and PC 2 send MLDv2 membership reports to join the multicast groups FF10::1 and FF50::1, respectively.

#Multicast Server sends multicast service packets of the multicast groups FF10::1 and FF50::1.

#View the multicast membership table on Device 3.

```
Device3#show ipv6 mld groups
MLD Connected Group Membership
Total 2 Connected Groups
Group   Interface   Uptime   Expires   V1-Expires   Last Reporter
ff10::1 vlan6       00:00:09 00:04:13  not used     fe80::210:94ff:fe00:1
ff50::1 vlan7       00:00:09 00:04:14  not used     fe80::210:94ff:fe00:2
```

#View the RPs corresponding to the multicast groups FF10::1 and FF50::1 on Device 3.

```
Device3#show ipv6 pim rp-hash ff10::1
PIM6 VRF Name: Default
RP: 2001:2::2
Info source: 2001:2::2, via bootstrap
```

```
Device3#show ipv6 pim rp-hash ff50::1
PIM6 VRF Name: Default
RP: 2001:3::1
Info source: 2001:2::2, via bootstrap
```

### #View the multicast routing table of Device 3.

```
Device3#show ipv6 pim mroute
IP Multicast Routing Table:
PIM6 VRF Name: Default
Total 0 (*,*,RP) entry
Total 2 (*,G) entries
Total 2 (S,G) entries
Total 2 (S,G,rpt) entries
Total 0 FCR entry
Up timer/Expiry timer
```

```
(*, ff10::1)
Up time: 00:00:06
RP: 2001:2::2
RPF nbr: fe80::201:7aff:fe62:bb7e
RPF idx: vlan3
Flags:
  JOIN DESIRED
Upstream State: JOINED
Local interface list:
  vlan6
Joined interface list:
Asserted interface list:
```

```
(2001:1::1, ff10::1)
Up time: 00:00:05
KAT time: 00:03:25
RPF nbr: fe80::201:7aff:fe62:bb7e
RPF idx: vlan3
SPT bit: TRUE
Flags:
  JOIN DESIRED
Upstream State: JOINED
Local interface list:
```

Joined interface list:  
Asserted interface list:  
Outgoing interface list:  
  vlan6  
Packet count 0

(2001:1::1, ff10::1, rpt)  
Up time: 00:00:05  
RP: 2001:2::2  
Flags:  
  RPT JOIN DESIRED  
  RPF SGRPT XG EQUAL  
Upstream State: NOT PRUNED  
Local interface list:  
Pruned interface list:  
Outgoing interface list:

(\*, ff50::1)  
Up time: 00:00:06  
RP: 2001:3::1  
RPF nbr: fe80::201:7aff:fec0:525a  
RPF idx: vlan5  
Flags:  
  JOIN DESIRED  
Upstream State: JOINED  
Local interface list:  
  vlan7  
Joined interface list:  
Asserted interface list:

(2001:1::1, ff50::1)  
Up time: 00:00:05  
KAT time: 00:03:27  
RPF nbr: fe80::201:7aff:fe62:bb7e  
RPF idx: vlan3  
SPT bit: TRUE  
Flags:  
  JOIN DESIRED  
Upstream State: JOINED  
Local interface list:

```
Joined interface list:
Asserted interface list:
Outgoing interface list:
  vlan7
Packet count 1

(2001:1::1, ff50::1, rpt)
Up time: 00:00:05
RP: 2001:3::1
Flags:
  RPT JOIN DESIRED
  PRUNE DESIRED
  RPF SGRPT XG EQUAL
Upstream State: PRUNED
Local interface list:
Pruned interface list:
Outgoing interface list:
  vlan7
```

#PC 1 can only receiver the multicast service packet of the multicast group FF10::1 sent by Multicast Server. #PC 2 can only receiver the multicast service packet of the multicast group FF50::1 sent by Multicast Server.

---

## Note

- Device1 and Device2 are checked in the same way as Device3, the process of which is omitted.
  - By default, SPT switching is enabled on the device.
- 

### 75.3.2 Configure IPv6 PIM-SSM

#### Network Requirements

- The IPv6 PIM-SSM protocol runs on the entire network.
- PC is one receiver of the Device 3 stub network.
- MLDv2 runs between Device 3 and the stub network.

#### Network Topology

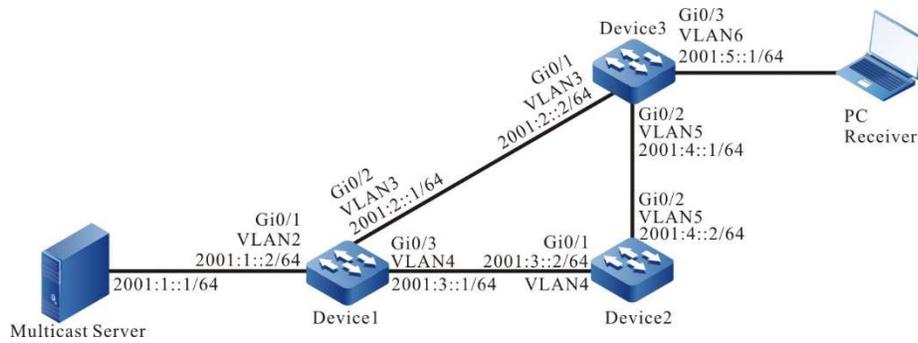


Figure 75-2 Network Topology for Configuring IPv6 PIM-SSM

### Configuration Steps

- Step 1: Configure VLANs, and add the port to the corresponding VLAN (omitted).
- Step 2: Configure the IPv6 address of each interface (omitted).
- Step 3: Enable the unicast routing protocol OSPFv3, so that all devices in the network can communicate with each other.

#### #Configure Device1.

```

Device1#configure terminal
Device1(config)#ipv6 router ospf 100
Device1(config-ospf6)#router-id 1.1.1.1
Device1(config-ospf6)#exit
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ipv6 router ospf 100 area 0
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan3
Device1(config-if-vlan3)#ipv6 router ospf 100 area 0
Device1(config-if-vlan3)#exit
Device1(config)#interface vlan4
Device1(config-if-vlan4)#ipv6 router ospf 100 area 0
Device1(config-if-vlan4)#exit

```

#### #Configure Device2.

```

Device2#configure terminal
Device2(config)#ipv6 router ospf 100
Device2(config-ospf6)#router-id 2.2.2.2
Device2(config-ospf6)#exit
Device2(config)#interface vlan4
Device2(config-if-vlan4)#ipv6 router ospf 100 area 0

```

```
Device2(config-if-vlan4)#exit
Device2(config)#interface vlan5
Device2(config-if-vlan5)#ipv6 router ospf 100 area 0
Device2(config-if-vlan5)#exit
```

### #Configure Device3.

```
Device3#configure terminal
Device3(config)#ipv6 router ospf 100
Device3(config-ospf6)#router-id 3.3.3.3
Device3(config-ospf6)#exit
Device3(config)#interface vlan3
Device3(config-if-vlan3)#ipv6 router ospf 100 area 0
Device3(config-if-vlan3)#exit
Device3(config)#interface vlan5
Device3(config-if-vlan5)#ipv6 router ospf 100 area 0
Device3(config-if-vlan5)#exit
Device3(config)#interface vlan6
Device3(config-if-vlan6)#ipv6 router ospf 100 area 0
Device3(config-if-vlan6)#exit
```

### #Check the routing table of Device3.

```
Device3#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management
```

```
L ::1/128 [0/0]
   via ::, 2w6d:04:39:46, lo0
O  2001:1::/64 [110/2]
   via fe80::201:7aff:fe62:bb7e, 00:00:24, vlan3
C  2001:2::/64 [0/0]
   via ::, 00:01:05, vlan3
L  2001:2::2/128 [0/0]
   via ::, 00:01:04, lo0
O  2001:3::/64 [110/2]
   via fe80::201:7aff:fe62:bb7e, 00:00:24, vlan3
   [110/2]
   via fe80::201:7aff:fec0:525a, 00:00:04, vlan5
C  2001:4::/64 [0/0]
   via ::, 00:00:49, vlan5
```

```
L 2001:4::1/128 [0/0]
  via ::, 00:00:48, lo0
C 2001:5::/64 [0/0]
  via ::, 00:00:43, vlan6
L 2001:5::1/128 [0/0]
  via ::, 00:00:42, lo0
```

---

## Note

- Device1 and Device2 are checked in the same way as Device3, the process of which is omitted.
- 

Step 4: Enable IPv6 multicast forwarding globally, and enable the multicast protocol IPv6 PIM-SM on the interfaces.

### #Configure Device1.

Enable IPv6 multicast forwarding globally, and enable the multicast protocol IPv6 PIM-SM on related interfaces.

```
Device1(config)#ipv6 multicast-routing
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ipv6 pim sparse-mode
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan3
Device1(config-if-vlan3)#ipv6 pim sparse-mode
Device1(config-if-vlan3)#exit
Device1(config)#interface vlan4
Device1(config-if-vlan4)#ipv6 pim sparse-mode
Device1(config-if-vlan4)#exit
```

### #Configure Device2.

Enable IPv6 multicast forwarding globally, and enable the multicast protocol IPv6 PIM-SM on related interfaces.

```
Device2(config)#ipv6 multicast-routing
Device2(config)#interface vlan4
Device2(config-if-vlan4)#ipv6 pim sparse-mode
Device2(config-if-vlan4)#exit
Device2(config)#interface vlan5
Device2(config-if-vlan5)#ipv6 pim sparse-mode
```

```
Device2(config-if-vlan5)#exit
```

### #Configure Device3.

Enable IPv6 multicast forwarding globally, and enable the multicast protocol IPv6 PIM-SM on related interfaces.

```
Device3(config)#ipv6 multicast-routing
Device3(config)#interface vlan3
Device3(config-if-vlan3)#ipv6 pim sparse-mode
Device3(config-if-vlan3)#exit
Device3(config)#interface vlan5
Device3(config-if-vlan5)#ipv6 pim sparse-mode
Device3(config-if-vlan5)#exit
Device3(config)#interface vlan6
Device3(config-if-vlan6)#ipv6 pim sparse-mode
Device3(config-if-vlan6)#exit
```

#View, for Device 3, interface information with IPv6 PIM-SM protocol enabled and IPv6 PIM-SM neighbor information.

```
Device3#show ipv6 pim interface
PIM6 Interface Table:
PIM6 VRF Name: Default
Total 4 Interface entries
Total 0 External Interface entry
Total 0 Sparse-Dense Mode Interface entry
```

```
Interface   VIF  Ver/ VIF  Nbr  DR  BSR  CISCO  Neighbor
           Index Mode  Flag Count Pri Border Neighbor Filter
register_vif0  2   v2/S UP   1   1   FALSE FALSE
Address : fe80::201:7aff:fe5e:6d2d  Global Address: ::

vlan3       1   v2/S UP   1   1   FALSE FALSE
Address : fe80::201:7aff:fe5e:6d2d  Global Address: 2001:2::2    DR: fe80::201:7aff:fe62:bb7e

vlan5       3   v2/S UP   1   1   FALSE FALSE
Address : fe80::201:7aff:fe5e:6d2e  Global Address: 2001:4::1    DR: fe80::201:7aff:fec0:525a

vlan6       4   v2/S UP   0   1   FALSE FALSE
Address : fe80::201:7aff:fe5e:6d2f  Global Address: 2001:5::1    DR: fe80::201:7aff:fe5e:6d2f
```

```
Device3#show ipv6 pim neighbor
PIM6 Neighbor Table:
PIM6 VRF Name: Default
```

Total 2 Neighbor entries

Neighbor Address	Interface	Uptime/Expires	Ver	DR
fe80::201:7aff:fe62:bb7e	vlan3	00:04:01/00:01:29	v2	1 / DR
fe80::201:7aff:fec0:525a	vlan5	00:04:03/00:01:39	v2	1 / DR

---

## Note

- Device1 and Device2 are checked in the same way as Device3, the process of which is omitted.
- 

Step 5: Enable MLD on vlan 6 of Device 3.

#Configure Device3.

Enable MLD on vlan 6 of Device 3.

```
Device3(config)#interface vlan6
Device3(config-if-vlan6)#ipv6 mld enable
Device3(config-if-vlan6)#exit
```

#View the MLD information of the interface vlan 6 of Device 3.

```
Device3#show ipv6 mld interface vlan6
Interface vlan6 (Index 11)
MLD Enabled, Active
Querier: fe80::201:7aff:fe5e:6d2f (Self)
Default version: 2
Querier parameter:
Query interval is 125 seconds
Querier timeout is 255 seconds
Query response time is 10 seconds
Last member query response interval is 1 seconds
Last member query count is 2
Group Membership interval is 260 seconds
Robustness variable is 2
```

---

## Note

- 
- By means of the command `ipv6 mld version` you can configure the version of IGMP that runs on the interface.
- 

Step 6: Configure IPv6 PIM-SSM on all devices. The range of multicast groups served by SSM is FF3X::/32.

#Configure Device1.

```
Device1(config)#ipv6 pim ssm default
```

#Configure Device2.

```
Device2(config)#ipv6 pim ssm default
```

#Configure Device3.

```
Device3(config)#ipv6 pim ssm default
```

Step 7: Check the result.

#PC sends the MLDv2 membership report of the specified source group to join the multicast group FF30::1, and the specified multicast source is 2001:1::1.

#Multicast Server sends the multicast service packet of the multicast group FF30::1.

#View the multicast membership table of Device 3.

```
Device3#show ipv6 mld groups detail
MLD Connected Group Membership
Total 1 Connected Groups
Group      Interface    Uptime   Expires  V1-Expires Last Reporter
ff30::1    vlan6        00:26:42 not used  not used  fe80::210:94ff:fe00:1
Group mode : Include
TIB-A Count: 1
TIB-B Count: 0

TIB-A
Source list: (R - Remote, M - SSM Mapping)
Source           Uptime   Expires  Flags
2001:1::1        00:05:55 00:03:41 R
```

#View the multicast routing table of Device 3.

```
Device3#show ipv6 pim mroute
IP Multicast Routing Table:
PIM6 VRF Name: Default
```

Total 0 (\*,\*,RP) entry  
Total 0 (\*,G) entry  
Total 1 (S,G) entry  
Total 0 (S,G,rpt) entry  
Total 0 FCR entry  
Up timer/Expiry timer

(2001:1::1, ff30::1)  
Up time: 00:06:48  
KAT time: 00:02:30  
RPF nbr: fe80::201:7aff:fe62:bb7e  
RPF idx: vlan3  
SPT bit: TRUE  
Flags:  
JOIN DESIRED  
Upstream State: JOINED  
Local interface list:  
vlan6  
Joined interface list:  
Asserted interface list:  
Outgoing interface list:  
vlan6  
Packet count 275560

#PC can only receive the multicast service packet of the multicast group FF30::1 sent by Source.

---

## Note

- Device 1 and Device 2 are viewed the same way as Device 3, and the viewing process is omitted.
  - The default multicast group range of IPv6 PIM-SSM is FF3X::/32. The range of multicast groups served by IPv6 PIM-SSM can be modified with the command `ipv6 pim ssm range`.
  - For the multicast group G that meets the SSM conditions, the multicast routing table will not generate entry (\*, G), but only entry (S, G).
-

## 75.3.3 Configure IPv6 PIM-SM Multicast Forwarding Control

### Network Requirements

- The IPv6 PIM-SM protocol runs on the entire network.
- PC is one receiver of the Device 3 stub network.
- Device 2 is C-BSR and C-RP.
- On Device 2 and Device 3, the multicast source is controlled so that PC can only receive the multicast service packet sent by Multicast Server 1.
- MLDv2 runs between Device 3 and the stub network.

### Network Topology

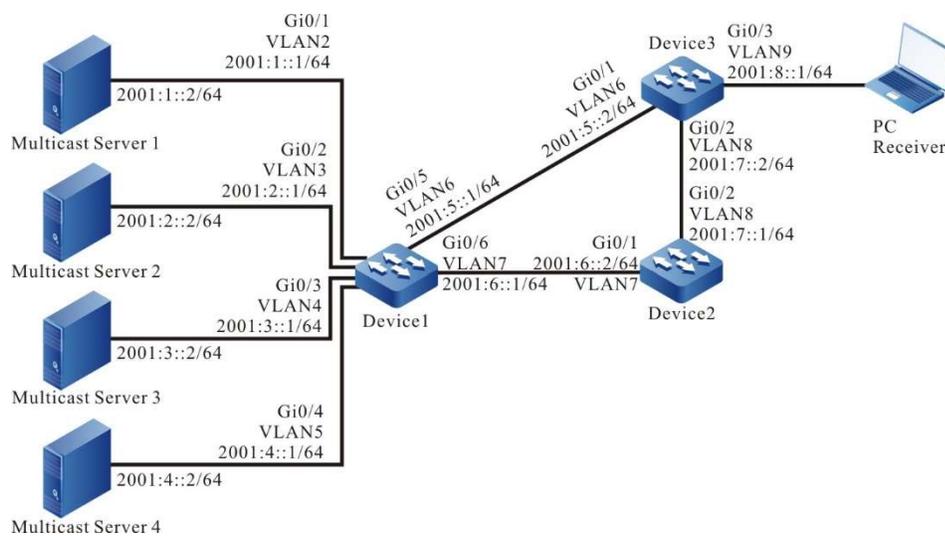


Figure 75-3 Network Topology for Configuring IPv6 PIM-SM Multicast Forwarding Control

### Configuration Steps

- Step 1: Configure VLANs, and add the port to the corresponding VLAN (omitted).
- Step 2: Configure the IPv6 address of each interface (omitted).
- Step 3: Enable the unicast routing protocol OSPFv3, so that all devices in the network can communicate with each other.

#### #Configure Device1.

```
Device1#configure terminal
Device1(config)#ipv6 router ospf 100
Device1(config-ospf6)#router-id 1.1.1.1
```

```
Device1(config-ospf6)#exit
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ipv6 router ospf 100 area 0
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan3
Device1(config-if-vlan3)#ipv6 router ospf 100 area 0
Device1(config-if-vlan3)#exit
Device1(config)#interface vlan4
Device1(config-if-vlan4)#ipv6 router ospf 100 area 0
Device1(config-if-vlan4)#exit
Device1(config)#interface vlan5
Device1(config-if-vlan5)#ipv6 router ospf 100 area 0
Device1(config-if-vlan5)#exit
Device1(config)#interface vlan6
Device1(config-if-vlan6)#ipv6 router ospf 100 area 0
Device1(config-if-vlan6)#exit
Device1(config)#interface vlan7
Device1(config-if-vlan7)#ipv6 router ospf 100 area 0
Device1(config-if-vlan7)#exit
```

### #Configure Device2.

```
Device2#configure terminal
Device2(config)#ipv6 router ospf 100
Device2(config-ospf6)#router-id 2.2.2.2
Device2(config-ospf6)#exit
Device2(config)#interface vlan7
Device2(config-if-vlan7)#ipv6 router ospf 100 area 0
Device2(config-if-vlan7)#exit
Device2(config)#interface vlan8
Device2(config-if-vlan8)#ipv6 router ospf 100 area 0
Device2(config-if-vlan8)#exit
```

### #Configure Device3.

```
Device3#configure terminal
Device3(config)#ipv6 router ospf 100
Device3(config-ospf6)#router-id 3.3.3.3
Device3(config-ospf6)#exit
Device3(config)#interface vlan6
Device3(config-if-vlan6)#ipv6 router ospf 100 area 0
Device3(config-if-vlan6)#exit
Device3(config)#interface vlan8
```

```
Device3(config-if-vlan8)#ipv6 router ospf 100 area 0
Device3(config-if-vlan8)#exit
Device3(config)#interface vlan9
Device3(config-if-vlan9)#ipv6 router ospf 100 area 0
Device3(config-if-vlan9)#exit
```

### #Check the routing table of Device3.

```
Device3#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management
```

```
L ::1/128 [0/0]
   via ::, 3w2d:05:13:23, lo0
O 2001:1::/64 [110/2]
   via fe80::201:7aff:fe62:bb7e, 00:00:24, vlan6
O 2001:2::/64 [110/2]
   via fe80::201:7aff:fe62:bb7e, 00:00:24, vlan6
O 2001:3::/64 [110/2]
   via fe80::201:7aff:fe62:bb7e, 00:00:24, vlan6
O 2001:4::/64 [110/2]
   via fe80::201:7aff:fe62:bb7e, 00:00:24, vlan6
C 2001:5::/64 [0/0]
   via ::, 00:01:52, vlan6
L 2001:5::2/128 [0/0]
   via ::, 00:01:50, lo0
O 2001:6::/64 [110/2]
   via fe80::201:7aff:fe62:bb7e, 00:00:24, vlan6
   [110/2]
   via fe80::201:7aff:fec0:525a, 00:00:24, vlan8
C 2001:7::/64 [0/0]
   via ::, 00:01:25, vlan8
L 2001:7::2/128 [0/0]
   via ::, 00:01:24, lo0
C 2001:8::/64 [0/0]
   via ::, 00:01:16, vlan9
L 2001:8::1/128 [0/0]
   via ::, 00:01:14, lo0
```

---

 **Note**

- Device 1 and Device 2 are viewed the same way as Device 3, and the viewing process is omitted.
- 

Step 4: Enable IPv6 multicast forwarding globally, and enable the multicast protocol IPv6 PIM-SM on the interfaces.

#### #Configure Device1.

Enable IPv6 multicast forwarding globally, and enable the multicast protocol IPv6 PIM-SM on related interfaces.

```
Device1(config)#ipv6 multicast-routing
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ipv6 pim sparse-mode
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan3
Device1(config-if-vlan3)#ipv6 pim sparse-mode
Device1(config-if-vlan3)#exit
Device1(config)#interface vlan4
Device1(config-if-vlan4)#ipv6 pim sparse-mode
Device1(config-if-vlan4)#exit
Device1(config)#interface vlan5
Device1(config-if-vlan5)#ipv6 pim sparse-mode
Device1(config-if-vlan5)#exit
Device1(config)#interface vlan6
Device1(config-if-vlan6)#ipv6 pim sparse-mode
Device1(config-if-vlan6)#exit
Device1(config)#interface vlan7
Device1(config-if-vlan7)#ipv6 pim sparse-mode
Device1(config-if-vlan7)#exit
```

#### #Configure Device2.

Enable IPv6 multicast forwarding globally, and enable the multicast protocol IPv6 PIM-SM on related interfaces.

```
Device2(config)#ipv6 multicast-routing
Device2(config)#interface vlan7
Device2(config-if-vlan7)#ipv6 pim sparse-mode
```

```

Device2(config-if-vlan7)#exit
Device2(config)#interface vlan8
Device2(config-if-vlan8)#ipv6 pim sparse-mode
Device2(config-if-vlan8)#exit

```

### #Configure Device3.

Enable IPv6 multicast forwarding globally, and enable the multicast protocol IPv6 PIM-SM on related interfaces.

```

Device3(config)#ipv6 multicast-routing
Device3(config)#interface vlan6
Device3(config-if-vlan6)#ipv6 pim sparse-mode
Device3(config-if-vlan6)#exit
Device3(config)#interface vlan8
Device3(config-if-vlan8)#ipv6 pim sparse-mode
Device3(config-if-vlan8)#exit
Device3(config)#interface vlan9
Device3(config-if-vlan9)#ipv6 pim sparse-mode
Device3(config-if-vlan9)#exit

```

#View, for Device 3, interface information with IPv6 PIM-SM protocol enabled and IPv6 PIM-SM neighbor information.

```

Device3#show ipv6 pim interface
PIM6 Interface Table:
PIM6 VRF Name: Default
Total 4 Interface entries
Total 0 External Interface entry
Total 0 Sparse-Dense Mode Interface entry

```

Interface	VIF	Ver/	VIF	Nbr	DR	BSR	CISCO	Neighbor
	Index	Mode	Flag	Count	Pri	Border	Neighbor	Filter
register_vif0	2	v2/S	UP					
Address : fe80::201:7aff:fe5e:6d2d Global Address: ::								
vlan6	1	v2/S	UP	1	1	FALSE	FALSE	
Address : fe80::201:7aff:fe5e:6d2d Global Address: 2001:5::2 DR: fe80::201:7aff:fe62:bb7e								
vlan8	4	v2/S	UP	1	1	FALSE	FALSE	
Address : fe80::201:7aff:fe5e:6d2e Global Address: 2001:7::2 DR: fe80::201:7aff:fec0:525a								
vlan9	3	v2/S	UP	0	1	FALSE	FALSE	
Address : fe80::201:7aff:fe5e:6d2f Global Address: 2001:8::1 DR: fe80::201:7aff:fe5e:6d2f								

```
Device3#show ipv6 pim neighbor
```

```
PIM6 Neighbor Table:
```

```
PIM6 VRF Name: Default
```

```
Total 2 Neighbor entries
```

Neighbor Address	Interface	Uptime/Expires	Ver	DR
fe80::201:7aff:fe62:bb7e	vlan6	00:07:08/00:01:25	v2	1 / DR
fe80::201:7aff:fec0:525a	vlan8	00:00:18/00:01:27	v2	1 / DR

---

## Note

- Device 1 and Device 2 are viewed the same way as Device 3, and the viewing process is omitted.
- 

Step 5: Configure vlan 7 of Device 2 as C-BSR and C-RP of the entire network. The range of multicast groups served by C-RP is FF00::/8.

### #Configure Device2.

```
Device2(config)#ipv6 pim bsr-candidate vlan7
```

```
Device2(config)#ipv6 pim rp-candidate vlan7
```

### #View the BSR and RP information of Device 3.

```
Device3#show ipv6 pim bsr-router
```

```
PIM6v2 Bootstrap information
```

```
PIM6 VRF Name: Default
```

```
BSR address: 2001:6::2
```

```
BSR Priority: 0
```

```
Hash mask length: 126
```

```
Up time: 00:00:21
```

```
Expiry time: 00:01:54
```

```
Role: Non-candidate BSR
```

```
State: Accept Preferred
```

```
Device3#show ipv6 pim rp mapping
```

```
PIM6 Group-to-RP Mappings Table:
```

```
PIM6 VRF Name: Default
```

```
Total 1 RP set entry
```

Total 1 RP entry

Group(s): ff00::/8

RP count: 1

RP: 2001:6::2

Info source: 2001:6::2, via bootstrap, priority 192

Up time: 00:00:28

Expiry time: 00:02:02

---

## Note

- Device 1 and Device 2 are viewed the same way as Device 3, and the viewing process is omitted.
- 

Step 6: On Device 2 and Device 3, the multicast source is controlled so that PC can only receive the multicast service packet sent by Multicast Server 1.

#On Device 2, configure the access list of accepted registration messages to filter out the registration messages of Multicast Server 4.

```
Device2(config)#ipv6 access-list extended 7001
Device2(config-std-nacl)#deny ipv6 host 2001:4::2 any
Device2(config-std-nacl)#permit ipv6 any any
Device2(config-std-nacl)#commit
Device2(config-std-nacl)#exit
Device2(config)#ipv6 pim accept-register list 7001
```

#Configure incoming IPv6 acl on interfaces vlan 6 and vlan 8 of Device 3 to filter out the multicast service packet of Multicast Server 3.

```
Device3(config)#ipv6 access-list extended 7001
Device3(config-v6-list)#deny ipv6 host 2001:3::2 any
Device3(config-v6-list)#permit ipv6 any any
Device3(config-v6-list)#commit
Device3(config-v6-list)#exit
Device3(config)#interface vlan6
Device3(config-if-vlan6)#ipv6 access-group 7001 in
Device3(config-if-vlan6)#exit
Device3(config)#interface vlan8
```

```
Device3(config-if-vlan8)#ipv6 access-group 7001 in
Device3(config-if-vlan8)#exit
```

#Configure outgoing IPv6 acl on interface vlan 9 of Device 3 to filter out the multicast service packet of Multicast Server 2.

```
Device3(config)#ipv6 access-list extended 7002
Device3(config-v6-list)#deny ipv6 host 2001:2::2 any
Device3(config-v6-list)#permit ipv6 any any
Device3(config-v6-list)#commit
Device3(config-v6-list)#exit
Device3(config)#interface vlan9
Device3(config-if-vlan9)#ipv6 access-group 7002 out
Device3(config-if-vlan9)#exit
```

Step 7: Check the result.

#PC sends an MLDv2 membership report to join the multicast group FF10::1.

#Multicast Server 1, Multicast Server 2, Multicast Server 3, Multicast Server 4 all send multicast service packets of the multicast group FF10::1.

#View the multicast membership table of Device 3.

```
Device3#show ipv6 mld groups
MLD Connected Group Membership
Total 1 Connected Groups
Group   Interface    Uptime   Expires  V1-Expires  Last Reporter
ff10::1 vlan9        00:35:31 00:03:31 not used    fe80::210:94ff:fe00:1
```

#View the multicast routing table of Device 3.

```
Device3#show ipv6 pim mroute
IP Multicast Routing Table:
PIM6 VRF Name: Default
Total 0 (*,*,RP) entry
Total 1 (*,G) entry
Total 2 (S,G) entries
Total 2 (S,G,rpt) entries
Total 0 FCR entry
Up timer/Expiry timer
```

```
(*, ff10::1)
Up time: 00:04:25
```

RP: 2001:6::2  
RPF nbr: fe80::201:7aff:fec0:525a  
RPF idx: vlan8  
Flags:  
JOIN DESIRED  
Upstream State: JOINED  
Local interface list:  
vlan9  
Joined interface list:  
Asserted interface list:

(2001:1::2, ff10::1)  
Up time: 00:03:33  
KAT time: 00:01:51  
RPF nbr: fe80::201:7aff:fe62:bb7e  
RPF idx: vlan6  
SPT bit: TRUE  
Flags:  
JOIN DESIRED  
Upstream State: JOINED  
Local interface list:  
Joined interface list:  
Asserted interface list:  
Outgoing interface list:  
vlan9  
Packet count 159075

(2001:1::2, ff10::1, rpt)  
Up time: 00:03:33  
RP: 2001:6::2  
Flags:  
RPT JOIN DESIRED  
PRUNE DESIRED  
RPF SGRPT XG EQUAL  
Upstream State: PRUNED  
Local interface list:  
Pruned interface list:  
Outgoing interface list:  
vlan9

(2001:2::2, ff10::1)  
Up time: 00:03:33  
KAT time: 00:01:51  
RPF nbr: fe80::201:7aff:fe62:bb7e  
RPF idx: vlan6  
SPT bit: TRUE  
Flags:  
JOIN DESIRED  
Upstream State: JOINED  
Local interface list:  
Joined interface list:  
Asserted interface list:  
Outgoing interface list:  
vlan9  
Packet count 156062

(2001:2::2, ff10::1, rpt)  
Up time: 00:03:33  
RP: 2001:6::2  
Flags:  
RPT JOIN DESIRED  
PRUNE DESIRED  
RPF SGRPT XG EQUAL  
Upstream State: PRUNED  
Local interface list:  
Pruned interface list:  
Outgoing interface list:  
vlan9

---

 **Note**

- Device 1 and Device 2 are viewed the same way as Device 3, and the viewing process is omitted.
- 

#Check the matching status of IPv6 acls on Device 2.

```
Device2#show ipv6 access-list 7001
ipv6 access-list extended 7001
10 deny ipv6 host 2001:4::2 any 14 matches
```

20 permit ipv6 any any 51 matches

#Check the matching status of IPv6 acls on Device 3.

```
Device3#show ipv6 access-list 7001
ipv6 access-list extended 7001
10 deny ipv6 host 2001:3::2 any 10760 matches
20 permit ipv6 any any 4089685 matches
```

```
Device3#show ipv6 access-list 7002
ipv6 access-list extended 7002
10 deny ipv6 host 2001:2::2 any 2046914 matches
20 permit ipv6 any any 2049595 matches
```

#PC can only receive the multicast service packet sent by Multicast Server 1.

---

## Caution

- When performing multicast source control, you are advised to configure multicast source control first and then demand the multicast source. By default, the receiving DR will switch SPTs after receiving the multicast service packet. If the multicast source is demanded before the multicast forwarding control is performed, the multicast forwarding control will not take effect. To prevent the multicast forwarding control from failing, you can configure SPT switching disallowed on the receiving DR.
- 

# 76 Hardware QoS

---

## 76.1 Overview

### 76.1.1 Background

In the traditional IP network, the forwarding device treats all packets equally, adopts “First in, first out” (FIFO) to process all packets and tries best effort to transmit the packet to the destination, so it cannot provide any guarantee for the reliability and delay of the packet transmission.

However, with the development of the IP network, the new applications based on the IP network emerge in endlessly, which put forward new requirements for the service quality of the IP network, especially the demand for the service packets with high real-time requirement is more obvious. For example, the network flow media, VoIP and other real-time services put forward high requirement for the transmission delay of the packets. If the packet transmission delay is long, the user cannot accept (relatively, E-mail and FTP services are not sensitive to the transmission delay). To support the communication services with different service quality requirements, it is required that the network can intelligently distinguish different communication types, so as to provide the corresponding service. The capability of distinguishing the communication types is the basic premise of providing different service qualities for different communications, so the best-effort service mode of the traditional IP network cannot meet the requirements of the present IP network application. The QoS (Quality of Service) technology is to solve the problem, so as to meet the different service quality requirements of the users for the network.

### 76.1.2 Service Model

QoS provides the following three kinds of service models, that is, Best-Effort service, Integrated service, and Differentiated service (DiffServ for short).

Best-Effort is a single service model and also the simplest service model. The application program can send out any quantity of packets at any time without getting the permission or informing the network in advance. For the best-effort service, the network tries best to send the packets, but does not provide any guarantee for the transmission delay and reliability of the packets. Best-Effort is the default service model of Internet and is applicable to most of network applications, such as FTP and E-Mail. It is realized via the FIFO queue mechanism.

IntServ is one service model that can provide various service types. It can meet various QoS requirements. Before sending packets, the service model needs to apply for the specified service resources from the network. The request is completed via the RSVP signaling. RSVP applies for the network resources for the application before the application program starts to send packets, so it belongs to the out-band signaling. Before sending data, the application program first informs the network of its own traffic parameters and the needed specified service quality request, including bandwidth, delay and so on. After receiving the resource request of the application program, the network executes the resource distributing check, that is, judge whether to distribute resources for the application program based on the resource application of the application program and the present

resources of the network. Once the network confirms to distribute resources for the application program, the network maintains one state for the specified flow (Flow, confirmed by the IP addresses, port numbers and protocol numbers of the two sides) and executes the packet classification, traffic monitoring, queuing and scheduling based on the state. After receiving the confirming information of the network (that is, confirm that the network already reserves resources for the packets of the application program), the application program can send packets. As long as the packets of the application program are controlled within the range described by the traffic parameters, the network will undertake to meet the QoS requirements of the application program.

DiffServ classifies the communications according to the service requirements, and then processes the ingress and egress packets according to the classification result, so as to ensure that the network is always in the good communication connection status. It is one multi-channel service model and can meet the QoS requirements of different flows. The largest difference with IntServ is that DiffServ can reserve resources in the network without signaling exchange. It just functions on one port of one transmission device in the network, processing the ingress and egress packets of the port. DiffServ does not need to maintain the status information for each kind of communication. It distinguishes the QoS level of each packet according to the configured QoS mechanism and provides the service for the packet according to the level. Therefore, the mechanism providing the QoS scheme is also called CoS. There are many classification methods and the common modes are to classify according to the priority of the IP packet, classify according to the source, destination address and port of the packet, classify according to the packet protocol, classify according to the packet size and packet ingress port, and so on.

Priority mapping, flow classification, traffic monitoring, traffic shaping, congestion management and congestion avoidance are the main components of DiffServ. The flow classification identifies the packets according to some matching rules and is the basis and premise of DiffServ; traffic monitoring, traffic shaping, congestion management and congestion avoidance distribute and schedule the resources for the network traffic from different aspects and they are the embodiment of the DiffServ idea.

### **76.1.3 Introduction to QoS Functions**

#### **Priority Mapping**

Priority mapping includes the ingress mapping and egress mapping. Ingress mapping maps to the local priority (LP) according to the 802.1p priority and DSCP value in the packet; egress mapping maps to the 802.1p priority and DSCP value according to the local priority (LP) of the packet. Priority mapping serves for the queue scheduling and congestion control.

The device supports four kinds of priority mapping: mapping the packet DSCP to the local priority (LP); mapping the 802.1p priority of the packet to the local priority (LP); mapping the local priority (LP) of the packet to the egress 802.1p priority of the packet; mapping the local priority (LP) of the packet to the egress DSCP value of the packet. The diagram of the priority mapping relation is as follows:

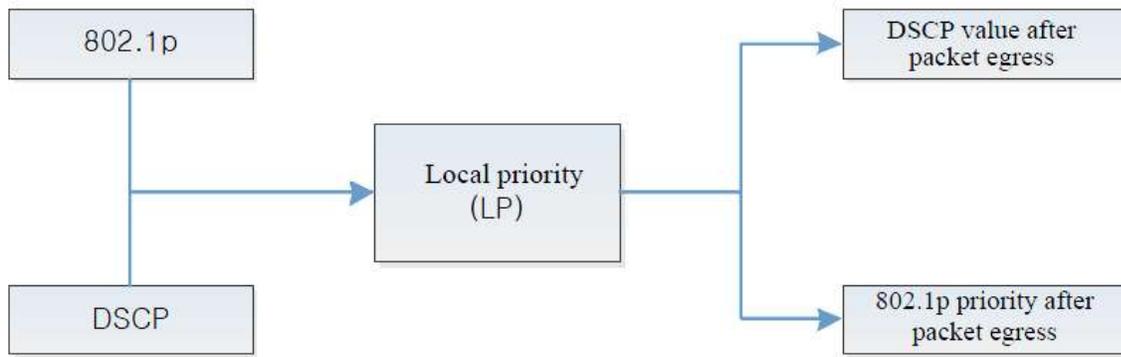


Figure 76-1 Diagram of Priority Mapping Relation

### Flow Classification

Flow classification adopts some rule to identify the packets that comply with one feature, divides the packets of different features to multiple classes, and then uses the corresponding QoS mechanism to provide different services for different classes. Therefore, the flow classification is the premise and basis of providing different services.

Flow classification includes counter, meter, flow mirror, redirection and re-remarking.

Counter and meter perform the counting and metering actions according to the result of the flow classification.

Flow mirror means to mirror the matched packets to the specified ports.

Redirection means to redirect the matched packets to the specified port or the specified next hop.

Re-marking means to set or modify the attributes of one kind of packets. After dividing the packets to different kinds via the flow classification, re-marking can modify the attributes of the packet. Prepare for the subsequent processing of the packet.

### Traffic Monitoring

Traffic monitoring limits the speed of the ingress packets via the token bucket. To ensure that the overload does not happen to the traffic passing the network and causes the congestion, the device provides the rate limitation based on the port receiving direction, limiting the total rate at the receiving direction of the port. The speeding traffic is dropped.

### Traffic Shaping

The typical function of the traffic shaping means to limit the traffic of flowing out from one network, making the packets sent with an average rate. Usually, it is divided to the port traffic shaping and queue traffic shaping. When the sending rate of the packets exceeds the shaping rate, the speeding packets are buffered in the queue and then are sent out with an average rate. The difference between the traffic shaping and traffic monitoring: When using the traffic monitoring to control the packet traffic, the speeding packets are not buffered, but are directly dropped, while the traffic shaping buffers the

speeding packets, reducing the dropped packets caused by the burst traffic. However, the traffic shaping may increase the delay, while the traffic monitoring nearly does not increase the delay.

### **Congestion Management**

When the device traffic load is light, do not generate the congestion and the packets are forwarded out when reaching the port. When the arriving rate of the packets is larger than the sending rate of the port and exceeds the processing limit of the port or the device resources are not enough, congestion happens to the device. The congestion may make the communication of the whole network become unreliable. The end-to-end delay, jitter and packet loss rate used to measure the network service quality all increase. If enabling the congestion management and when the congestion happens, the packets queue at the port and waits for the port to forward. The congestion management usually adopts the queue technology and the port determines which queue the packet should be placed according to the packet priority and queue mechanism and how to schedule and forward packets.

The common scheduling includes SP (Strict Priority), RR (Round Robin), and WDRR (Weighted Deficit Round Robin).

SP (Strict Priority): There are eight queues on the port, queue 0-7. Queue 7 has the highest priority and queue 0 has the lowest priority.

RR (Round Robin): After one queue schedules one packet, turn to the next queue.

WDRR (Weighted Deficit Round Robin): The algorithm is based on two variables, that is, quantum and credit counter. The quantum means the weight in the unit of byte and it is a configurable parameter. The credit counter means the accumulation and consumption of the quantum, which is a status parameter and cannot be configured. In the initial state, the credit counter of each queue is equal to the quantum. Every time the queue sends a packet, subtract the byte number of the packet from the credit counter. When the credit counter is lower than 0, stop the scheduling of the queue. When all queues stop scheduling, supplement quantum for all queues.

### **Congestion Avoidance**

The congestion avoidance technology monitors the communication load of the network, so as to avoid the congestion before the network congestion happens. The common used technology is WRED (Weighted Random Early Detection). The difference with the tail drop method is that WRED selects the dropped packet according to the DSCP or IP priority and can provide different performance features for different service types of data. It also can avoid the TCP global synchronization.

In the WRED algorithm, the start point of the queue drop packet is marked as DropStartPoint and the end point of the drop is marked as DropEndPoint. When the average length of the queue is between DropStartPoint and DropEndPoint, WRED drops the packet at random by the corresponding drop rate, while when the queue length exceeds DropEndPoint, drop the packet by 100%. When the queue length is smaller than DropStartPoint, WRED does not drop the packet.

The following figure is a schematic diagram on How WRED Works:

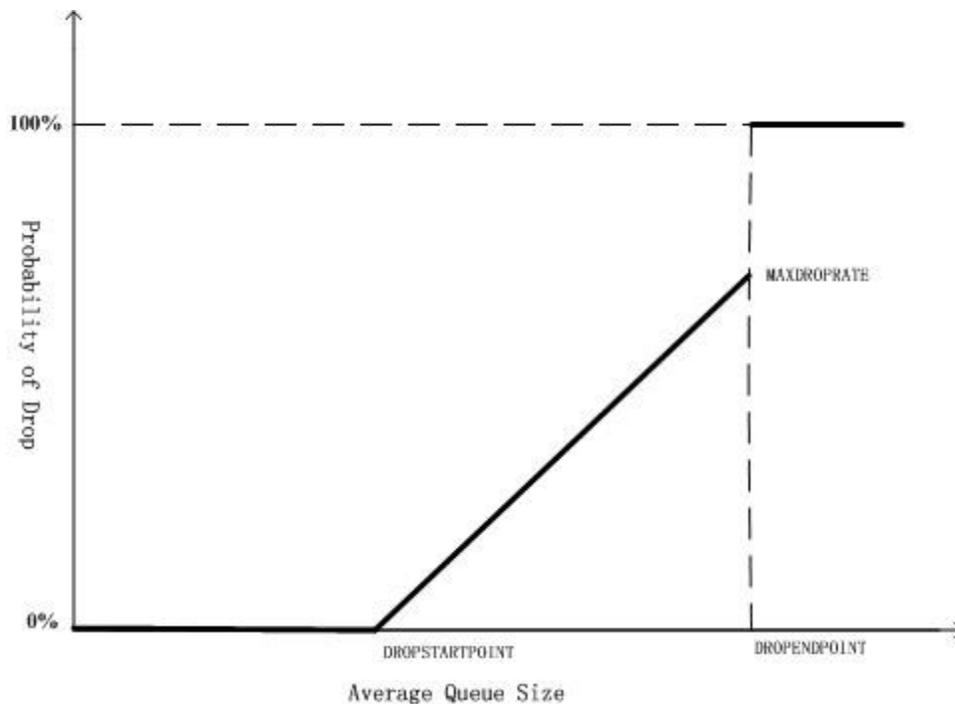


Figure 76-2 Schematic Diagram on How WRED Works

### Action Group Function

To support the flow classification and traffic control, the device extends the traditional ACL so that ACL and ACL rule can be bound with one action group respectively, adopting the corresponding action for the matched packet. The action group contains the configurations of the counter, meter, flow mirror, redirection and remarking.

For various ACLs and ACL rules being used in different function domains, the configurations of the action groups are different. For the ingress ACL, the used action group of IP ACL is L3 action group and the used action group of MAC ACL is L2 action group. The egress action group is used at the egress direction of ACL. The VFP action group is used to realize the flow-based QinQ. Each ACL can be bound with various action groups, but the effective one depends on the function domain bound with the ACL. For example, one rule of IP ACL is configured with L3 action group, egress action group and VFP action group at the same time. When the IP ACL is applied at the ingress direction, the action in the L3 action group take effect and the actions in the other two action groups do not take effect.

The policy route in the action group is one packet forwarding mechanism for flexible routing based on the destination network. The policy route classifies the packets via Content Aware Processor and forwards the data flow that complies with the classification rule according to the specified next hop. When some packet is routed by other path, but not the shortest path, we can enable the policy route. The policy route can be enabled when some packets need to be routed by other paths instead of the clear shortest path. The priority of the policy route is higher than any other route. Therefore, once the user configures enabling the policy route, the packet sending is processed according to the policy route. Only when the access list matching fails, we can continue to forward according to the searching result of the forwarding table. Otherwise, forward the packet according to the specified next-hop information of

the route policy. The specified next hop of the policy route should be the direct-connected next hop. For the non-direct-connected next-hop address, the system permits to configure, but in fact, it is invalid.

## 76.2 Hardware QoS Function Configuration

Table 76-1 Hardware QoS Function Configuration List

Configuration Task	
Configure Priority Mapping	Configure Priority Mapping
	Configure Default Priority Mapping
Configure Flow Classification	Configure Counter
	Configure Meter
	Configure Flow Mirror
	Configure Redirection
	Configure Re-marking I2-priority
	Configure Re-marking I3-priority
Configure Traffic Monitoring	Configure Port-based Rate Limitation
Configure Traffic Shaping	Configure Queue-based Traffic Shaping
	Configure Port-based Traffic Shaping
Configure Congestion Management	Configure Scheduling Policy of Port Queue
Configure Congestion Avoidance	Configure Drop Mode
Configure VFP Action Group	Configure Processing of Single VLAN Tag Packets
	Configure Processing of Double VLAN Tag Packets
	Configure Processing of Packets without VLAN Tags

Configuration Task	
	Configure Binding of VRF in VFP Action Group
Configure Priority-Based Flow Control	Configure Priority-Based Flow Control
Configure explicit congestion notification	Configure explicit congestion notification

### 76.2.1 Configure Priority Mapping

Priority mapping is the mapping among the 802.1p priority, DSCP value and local priority (LP) in the packet. Modify or distribute the priority field of the packet to serve for the congestion avoidance and congestion management.

#### Configuration Condition

None

#### Configure Priority Mapping

Priority mapping includes the ingress mapping and egress mapping. The ingress mapping maps to the local priority (LP) according to the 802.1p priority and DSCP value in the packet; the egress mapping maps to the 802.1p priority and DSCP value according to the local priority (LP).

Table 76-2 Configuring Priority Mapping

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure priority mapping template	<b>qos map-table {ingress   egress } <i>template-name</i></b>	Mandatory Configure egress and ingress priority templates

Step	Command	Description
Enter the template view	<b>{ dot1p-lp   dscp-lp   lp-dot1p   lp-dscp } index to value</b>	Optional By default, priority mapping under the template is default mapping relation
Binding the priority mapping template to the port	<b>map-table template-name { ingress   egress }</b>	Mandatory By default, no priority mapping template is bound

 说明:

- For the packet with the specified priority entering the queue, you'd better not let the packet enter queue 7, because the packets sent out from CPU all enter queue 7. If queue 7 has too many packets, the packets from CPU may be dropped.
- The dscp-lp mapping and dot1p-lp are configured on the port at the same time. The dscp-lp has higher priority and it takes effect first.
- After enabling the ingress dot1p-lp mapping, the 802.1p priority of the forwarded packet is modified according to the local priority (LP) by default. For example, the dot1p-lp mapping relation is 1 to 5; after matching the 802.1p of the VLAN Tag in the ingress packet to 1, the 802.1p priority of the forwarded packet with VLAN Tag is modified to 5.
- The priority mapping does not take effect for the packet remarked by the action group. First, remark the local priority (LP) at the ingress action group, and then mapping to the 802.1p priority and DSCP value of the packet via the local priority (LP) at the egress takes effect. Remark the 802.1p priority at the ingress and then mapping the local priority and DSCP value via the 802.1p priority does not take effect, but remarking the 802.1p priority itself takes effect. Mapping according to the 802.1p priority of the original packet also takes effect. That is to say, remarking takes effect separately, the priority mapping takes effect separately, and the priority mapping according to the remarked value does not take effect.
- If the QINQ function is enabled on the port, and the template bound to the port includes dot1p-lp and dscp-lp mappings, maybe you cannot get the desired mapping result. Therefore, it is recommended not to enable QinQ and bind the priority mapping function on one port at the same time.
- After configuring the lp-dscp mapping, the default mapping of lp-dscp is 0 to 7, 1 to 8, 2 to 16, 3 to 24, 4 to 32, 5 to 40, 6 to 48, and 7 to 56.

## Configure Default Priority Mapping

The default priority mapping, the same as the priority mapping, has the ingress and egress mapping. The difference lies in that the default priority mapping maps the entries not configured with priority mapping to the default value.

Table 76-3 Configuring Default Priority Mapping

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure priority mapping template	<b>qos map-table {ingress   egress } <i>template-name</i></b>	Mandatory Configure egress and ingress priority templates
Configure Default Priority Mapping	<b>{ dot1p-lp   dscp-lp   lp-dot1p   lp-dscp } default <i>value</i></b>	Mandatory By default, no default priority mapping is configured

### 76.2.2 Configure Flow Classification

Flow classification adopts some rule to identify the packets that comply with one feature, divides the packets of different features to multiple classes, and then uses the corresponding QoS mechanism to provide different services for different classes. Therefore, the flow classification is the premise and basis of providing different services.

#### Configuration Condition

Before configuring the flow classification, first complete the following task:

- Configure the ACL.

#### Configure Counter

Configuring counting action in the action group aims to count the number of the matched packets.

Table 76-4 Configuring the Counter

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure L3 action group and enter L3 action group configuration mode	<b>l3-action-group</b> <i>l3-action-group-name</i>	At least one option must be selected.  The subsequent configuration takes effect only on the current L3 action group after you enter the L3 action group configuration mode, only on the current L2 action group after you enter the L2 action group configuration mode, only on the current egress action group after you enter the egress action group configuration mode
Configure L2 action group and enter L2 action group configuration mode	<b>l2-action-group</b> <i>l2-action-group-name</i>	
Configure egress action group and enter egress action group configuration mode	<b>egr-action-group</b> <i>egr-action-group-name</i>	
Configure Counter	<b>count { all-colors }</b>	Mandatory  By default, packets are not counted in the action group

## Configure Meter

Configure the meter in the action group to limit the rate or mark the matched packets. When configuring a nonexistent meter, the meter takes effect immediately when the specified meter is configured. When no meter is configured in the action group, all matched packets are considered as green packets. When a meter is configured in the action group for coloring the packets, the packets will be marked in green, yellow, and red according to the packet traffic, and then the counter will count the number of the packets of different colors.

Table 76-5 Configuring Meter

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the meter and enter the meter mode	<b>traffic-meter</b> <i>traffic-meter-name</i>	Mandatory  By default, the action for yellow packets in the meter is drop, and the meter mode is not configured  After entering the meter configuration, one complete meter configuration contains the meter action for yellow packets and meter mode configuration, and the incomplete configuration will not take effect
Configure meter action	<b>meter action {yellow   red} { drop   transmit }</b>	Optional  By default, the action for yellow packets in the meter is drop
Configure meter mode	<b>meter mode { srtcm cir cbs ebs   trtcm cir cbs pir pbs }</b>	Mandatory  By default, the meter mode is not configured
Enter the global configuration mode.	<b>exit</b>	-
Configure L3 action group and enter L3 action group configuration mode	<b>l3-action-group</b> <i>l3-action-group-name</i>	At least one option must be selected.  The subsequent
Configure L2 action group and enter L2 action group configuration mode	<b>l2-action-group</b> <i>l2-action-group-name</i>	configuration takes effect only on the current L3 action group after you enter the L3 action group

Step	Command	Description
Configure egress action group and enter egress action group configuration mode	<b>egr-action-group</b> <i>egr-action-group-name</i>	configuration mode, only on the current L2 action group after you enter the L2 action group configuration mode, only on the current egress action group after you enter the egress action group configuration mode
Configure to bind the meter	<b>meter</b> <i>traffic-meter-name</i>	Mandatory  By default, no meter is bound

 说明:

- If the ACL bound to the objects is configured with the action group and the action group is configured with a meter for limiting the rate, conflicted rate limitation actions may exist. When the rate limitation is applied, the packets in red and yellow are dropped. For example, port 0/1 belongs to VLAN 1, ACL on port 0/1 permits the packets with the source IP address 1.1.1.1 to pass, and the action to limit its traffic to 5Mbps is configured. Whereas, ACL on VLAN 1 permits the packets with the IP address 1.1.1.1 to pass, and the action to limit its traffic to 1Mbps is configured. In this situation, the minimum rate in the packet channel will take effect and the traffic is configured within 1 Mbps. Specially, due to the hardware limitation, the actual traffic for multi-level rate limitation will be less than the minimum rate in the packet channel. Therefore, multi-level rate limitation is not recommended when an accurate rate limitation is needed.
- The meter in the egress action group does not support the remark lp or remark dotlp-lp action.
- Remarking of yellow packets is not supported.
- The meter is based on the chips. That is, the meter on each chip limits the traffic rate over the port. If the meter exists in two different chips under the link aggregation port, a meter exists in each chip and thus the rate limitation has the effect twice of the expected rate limitation effect.
- If a meter is applied to the VLAN, the meter takes effect for each chip on each line card. VLAN objects are limited within 10 Mbps. If five single-core line cards exist on the device, the 10 Mbps traffic takes effect for a pair of line cards. That is, the traffic on each line card complying with the VLAN rate limitation is 10 Mbps. If two chips exist on a line card, the traffic for each chip on the line card is 10 Mbps.

## Configure Flow Mirror

Configuring the flow mirror in the action group aims to specify the matched packet to the port.

Table 76-6 Configuring Flow Mirror

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure L3 action group and enter L3 action group configuration mode	<b>l3-action-group</b> <i>l3-action-group-name</i>	At least one option must be selected.  The subsequent configuration takes effect only on the current L3 action group after you enter the L3 action group configuration mode, and only on the current L2 action group after you enter the L2 action group configuration mode
Configure L2 action group and enter L2 action group configuration mode	<b>l2-action-group</b> <i>l2-action-group-name</i>	
Configure Flow Mirror	<b>mirror interface</b> <i>interface-name</i>	Mandatory  By default, no flow mirror is configured

## Configure Redirection

Configuring the packet redirection in the action group aims to redirect the matched packets to the specified port or the specified next hop.

Table 76-7 Configuring Redirection

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Configure L3 action group and enter L3 action group configuration mode	<b>I3-action-group</b> <i>l3-action-group-name</i>	At least one option must be selected.  The subsequent configuration takes effect only on the current L3 action group after you enter the L3 action group configuration mode, and only on the current L2 action group after you enter the L2 action group configuration mode
Configure L2 action group and enter L2 action group configuration mode	<b>I2-action-group</b> <i>l2-action-group-name</i>	
Configure Redirection	<b>redirect { interface</b> <i>interface-name</i> <b>  interface link-aggregation</b> <i>link-aggregation-id</i> <b>}</b>	Mandatory  By default, no packet redirection is configured

### Configure Re-marking I2-priority

Configuring packet remarking in the action group aims to classify the matched packets. So users are allowed to adopt different QoS policies in the subsequent data communications.

Table 76-8 Configuring Remarking I2-priority

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure L3 action group and enter L3 action group configuration mode	<b>I3-action-group</b> <i>l3-action-group-name</i>	At least one option must be selected.  The subsequent configuration takes effect only on the current L3 action group after you enter the L3 action group
Configure L2 action group and enter L2 action group configuration mode	<b>I2-action-group</b> <i>l2-action-group-name</i>	

Step	Command	Description
Configure egress action group and enter egress action group configuration mode	<b>egr-action-group</b> <i>egr-action-group-name</i>	configuration mode, only on the current L2 action group after you enter the L2 action group configuration mode, only on the current egress action group after you enter the egress action group configuration mode
Configure Re-marking l2-priority	<b>remark l2-priority</b> { <b>dscp</b> <i>dscp-value</i>   {{ <b>dot1p</b>   <b>dot1p-lp</b>   <b>lp</b> }} { <i>priority-value</i>   <b>precedence</b> }}	Mandatory  By default, remarking l2-priority is not configured

 说明:

- The action group does not support using the priority field in the IP packet TOS to remark the 802.1p priority in the VLAN Tag.
- The egress action group does not support the remark action.

### Configure Re-marking l3-priority

Configuring packet remarking in the action group aims to classify the matched packets. So users are allowed to adopt different QoS policies in the subsequent data communications.

Table 76-9 Configuring Remarking l3-priority

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure L3 action group and enter L3 action group configuration mode	<b>l3-action-group</b> <i>l3-action-group-name</i>	At least one option must be selected.  The subsequent configuration takes effect only on the current L3 action group after you
Configure egress action group and enter egress	<b>egr-action-group</b> <i>egr-action-group-name</i>	

Step	Command	Description
action group configuration mode		enter the L3 action group configuration mode, and only on the current egress group after you enter the egress action group configuration mode
Configure Re-marking I3-priority	<b>remark I3-priority { dscp dscp-value   precedence { priority-value   dot1p }}</b>	Mandatory By default, remarking I3-priority is not configured

 说明:

- If the ACL bound to the objects is configured with the action group, re-marking confliction may exist. For example, port 0/1 belongs to VLAN1, the ACL on port 0/1 permits the packets of the source IP address 1.1.1.1 to pass, and the action for re-marking the DSCP field as 5 is configured. The ACL of VLAN 1 permits the packets of the IP address 1.1.1.1 to pass and the action for remarking the DSCP field as 4 is configured. In this situation, this situation is handled based on port > VLAN > global and MAC ACL > IP ACL by priority and the final remarking value is 5.
- If the ACL bound to the objects is configured with the action group, conflict-free re-marking action may exist. For example, port 0/1 belongs to VLAN1, the ACL on port 0/1 permits the packets of the source IP address 1.1.1.1 to pass, and the action for re-marking the DSCP field as 5 is configured. The ACL of VLAN 1 permits the packets of the IP address 1.1.1.1 to pass and the 802.1p priority is re-marked as 4. For the conflict-free remarking action, the packet DSCP will be marked as 5 and the 802.1p priority will be marked as 4.
- The action group does not support using the 802.1p priority in the VLAN Tag to remark the priority field in the IP packet TOS.
- The egress action group does not support the remark action.

### 76.2.3 Configure Traffic Monitoring

To ensure that the overload does not happen to the traffic passing the network and causes the congestion, the device provides the rate limitation based on the port receiving direction, limiting the total rate at the receiving direction of the port. The speeding traffic is dropped.

#### Configuration Condition

None

### Configure Port-based Rate Limitation

To provide different rate limitations for ports at different time periods, each port is configured with eight rate limitations of different priorities. Each rate is limited and then bound to a time domain. For the entries taking effect at the same time, determine which entry takes effect by priority. The number 0 indicates the highest priority and the number 7 indicates the lowest priority. The rate limitation over the port can be configured directly without the time domain.

Table 76-10 Configuring Port-based Rate Limitation

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the L2/L3 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	-
Configure port-based rate limiting	<b>rate-limit</b> { <b>default rate</b> <i>burst-size</i>   <i>priority rate</i> <i>burst-size</i> [ <b>time-range</b> <i>time-range-name</i> ] }	Mandatory By default, no flow limit is configured on the port

## 76.2.4 Configure Traffic Shaping

The traffic shaping enables the packets to be sent out at an average rate. The difference between the traffic shaping and traffic monitoring: the traffic monitoring takes effect in the ingress direction and the traffic shaping takes effect in the egress direction. The excessive traffic at the ingress direction will be dropped, but the excessive traffic at the egress direction will be cached.

### Configuration Condition

None

### Configure Queue-based Traffic Shaping

Queue-based traffic shaping enables the traffic in the queue to be sent out at an average rate. Different traffic shaping can be performed for different queues as required.

Table 76-11 Configuring Queue-based Traffic Shaping

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the L2/L3 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	-
Configure Queue-based Traffic Shaping	<b>traffic-shape queue</b> <i>queue-id</i> { { <b>cir</b> <i>cir</i> [ <b>cbs</b> <i>cbs</i> ] <b>pir</b> <i>pir</i> [ <b>pbs</b> <i>pbs</i> ] }   { <b>cir</b> <i>cir</i> [ <b>cbs</b> <i>cbs</i> ] }   { <b>pir</b> <i>pir</i> [ <b>pbs</b> <i>pbs</i> ] } }	Mandatory  By default, queue-based traffic shaping is not configured

### Configure Port-based Traffic Shaping

The port-based traffic shaping allows the time domain binding to achieve different bandwidths in different time periods. Each port is configured with eight traffic shaping of different priorities and each traffic shaping is bound to a time domain. For the entries taking effect at the same time, determine which entry takes effect by priority. The number 0 indicates the highest priority and the number 7 indicates the lowest priority.

Table 76-12 Configuring Port-based Traffic Shaping

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	-
Configure Port-based Traffic Shaping	<b>traffic-shape</b> { { <b>pir</b> <i>rate</i> [ <b>pbs</b> <i>burst-size</i> ] } / { <i>priority</i> <b>pir</b> <i>rate</i> [ <b>pbs</b>	Mandatory

Step	Command	Description
	<i>burst-size</i> ][ <b>time-range</b> <i>range-name</i> ] } }	By default, queue-based traffic shaping is not configured on the port

## 76.2.5 Configure Congestion Management

In a complex network, congestion is common because the current bandwidth cannot satisfy the normal forwarding. Congestion may cause a series of negative problems as follows: the system breaks down because of abundant network resources, the network resource utility is low because of decreased network throughput, and packet transmission delay and jitter increase. Scheduling policy for the port queue is a method for managing the congestion.

### Configuration Condition

None

### Configure Scheduling Policy of Port Queue

The queue-based scheduling policy sends out the classified traffic by a certain priority-level algorithm. Each queue algorithm solves a certain network traffic problem and has great influence on bandwidth resource allocation, delay, and jitter. Queue scheduling processes the packets of different priorities in levels. A packet with high priority will be sent preferentially.

The common scheduling includes SP (Strict Priority), RR (Round Robin) and WDRR (Weighted Deficit Round Robin).

SP (Strict Priority): There are eight queues on the port, queue 0-7. Queue 7 has the highest priority and queue 0 has the lowest priority.

RR (Round Robin): After one queue schedules one packet, turn to the next queue; WRR is Weighted Round Robin. You can configure the number of the packets scheduled by each queue before turning to the next queue;

WDRR (Weighted Deficit Round Robin): The algorithm is based on two variables, that is, quantum and credit counter. The quantum means the weight in the unit of byte and it is a configurable parameter. The credit counter means the accumulation and consumption of the quantum, which is a status parameter and cannot be configured. In the initial state, the credit counter of each queue is equal to the quantum. Every time the queue sends a packet, subtract the byte number of the packet from the credit counter. When the credit counter is lower than 0, stop the scheduling of the queue. When all queues stop scheduling, supplement quantum for all queues.

Table 76-13 Configuring Scheduling Policy of Port Queue

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the L2/L3 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	-
Configure Scheduling Policy of Port Queue	<b>queue-schedule</b> { <b>sp</b>   <b>rr</b>   {{ <b>wdr</b>   <b>wrr</b> } <i>weight0</i> <i>weight1 weight2 weight3</i> <i>weight4 weight5 weight6</i> <i>weight7</i> }}	Mandatory  By default, strict priority (SP) scheduling is used as the scheduling policy of port queue

## 76.2.6 Configure Congestion Avoidance

The congestion avoidance technology monitors the network resource utility and communication load of the network, so as to avoid the congestion by actively dropping packets before the network congestion happens or worsens. Excessive congestion exerts great harm on network resources and therefore, a certain measure must be adopted to relieve the congestion. The common measure is to configure the packet drop mode.

### Configuration Condition

None

### Configure Drop Mode

Tail drop and WRED (Weighted Random Early Detection) are two common packet drop modes.

**Tail drop:** It is a traditional packet drop policy. When the queue length reaches the maximum value, all new packets will be dropped. This packet drop policy may cause TCP global synchronization. When the packets connected by multiple TCPs are dropped in a queue, multiple TCP connections will enter the congestion avoidance and slow-start status to decrease and adjust the traffic, and then the traffic peak may occur simultaneously at a time. Repeatedly, the traffic and network are unstable.

**WRED:** When the queue length exceeds its own length, the packets are dropped by 100%. When the queue length is less than the start-value, do not drop any packet. When the queue length is greater than the start-value, drop packets at random according to the configured value. The random number generated by the WRED is based on the priority. The WRED introduces the IP priority to distinguish from

the packet drop policy. The packet with high priority is considered for its benefit and this packet will be dropped in a relatively low probability.

Table 76-14 Configuring Drop Mode

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	-
Configure Drop Mode	<b>drop-mode</b> <i>cos-value</i> { <b>tail-drop</b>   <b>wred drop-start</b> <i>start-value</i> <b>drop-rate</b> <i>drop-rate-value</i> [ <b>only-tcp</b>   <b>all</b> ] }	Mandatory  By default, the drop mode of port queue is tail-drop

### 76.2.7 Configure VFP Action Group

The VFP (VLAN Filter Processor) action group involves actions used to classify packets and re-specify single VLAN Tag packets, double VLAN Tag packets, and packets without VLAN tags.

#### Configuration Condition

Before configuring the VFP action group, do the following:

- Configure the ACL.

#### Configure Processing of Single VLAN Tag Packets

Configuring processing of single VLAN Tag packets in the VFP action group is mainly concerned with matching and processing of the 802.1P priorities and VLAN numbers in the VLAN Tags.

Table 76-15 Configuring Processing of Single VLAN Tag Packets

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Configure the VFP action group and enter the VFP action group configuration mode	<b>vfp-action-group</b> <i>vfp-action-group-name</i>	Mandatory  By default, no VFP action group is configured
Configure Processing of Single VLAN Tag Packets	<b>one-tag</b> { <b>match-vlan</b> { <b>any</b>   <i>vlan-id</i> }   <b>ovlan-act</b> { <b>add-ovlan</b> <i>vlan-id</i> [ <b>priority</b> <i>priority-value</i> ] }   <b>replace-vlan</b> <i>vlan-id</i> }	Mandatory  By default, processing of single VLAN Tag packets is not configured

### Configure Processing of Double VLAN Tag Packets

Configuring processing of double VLAN Tag packets in the VFP action group is mainly concerned with matching and processing of the 802.1P priorities and VLAN numbers in the inner and outer VLAN Tags.

Table 76-16 Configuring Processing of Double VLAN Tag Packets

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the VFP action group and enter the VFP action group configuration mode	<b>vfp-action-group</b> <i>vfp-action-group-name</i>	Mandatory  By default, no VFP action group is configured
Configure Processing of Double VLAN Tag Packets	<b>double-tag</b> { <b>invlan-act</b> { <b>delete-invlan</b>   <b>replace-invlan</b> <i>vlan-id</i> }   <b>match-invlan</b> { <b>any</b>   <i>vlan-id</i> }   <b>match-ovlan</b> { <b>any</b>   <i>vlan-id</i> }   <b>ovlan-act</b> <b>replace-ovlan</b> <i>vlan-id</i> }	Mandatory  By default, processing of double VLAN Tag packets is not configured

### Configure Processing of Packets without VLAN Tags

Configuring processing of packets without VLAN tags in the VFP action group is mainly concerned with configuring the addition of actions into the inner and outer VLAN Tags.

Table 76-17 Configuring Processing of Packets without VLAN Tags

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the VFP action group and enter the VFP action group configuration mode	<b>vfp-action-group</b> <i>vfp-action-group-name</i>	Mandatory By default, no VFP action group is configured
Configure Processing of Packets without VLAN Tags	<b>untag { invlan-act add- invlan <i>vlan-id</i> }   ovlan-act add-ovlan <i>vlan-id</i></b>	Mandatory By default, processing of packets without VLAN Tags is not configured

### Configure Binding of VRF in VFP Action Group

Table 76-18 Configuring Binding of VRF in VFP Action Group

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the VFP action group and enter the VFP action group configuration mode	<b>vfp-action-group</b> <i>vfp-action-group-name</i>	Mandatory By default, no VFP action group is configured
Configure Binding of VRF in VFP Action Group	<b>vrfset <i>vrf-name</i></b>	Mandatory By default, binding VRF is not performed in the VFP action group

## 76.2.8 Configure explicit congestion notification

In the case of explicit congestion notification, when congestion occurs on the device, the ECN field in the header of IP packets is marked. Then, the receiving end sends Congestion Notification Packets (CNP packets) to the sending end to alleviate congestion and implement end-to-end congestion management

### Configuration Condition

None

### Configure explicit congestion notification

In the case of ECN (Explicit Congestion Notification), it defines a traffic control and end-to-end congestion notification mechanism based on IP layer and transport layer. The ECN function uses the DS field in the IP packet header to mark the congestion status on the packet transport path. The terminal device that supports this function can identify congestion on the transport path based on the packet content and adjust the sending mode of packets to avoid intensified congestion.

Table 76-19 Configuring Explicit Congestion Notification Function Of Device

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Turn on the explicit congestion notification function	<b>ecn</b>	-

## 76.2.9 Configure Traffic Flooding

By default, unknown broadcast, unknown multicast, and unknown unicast packets will flood in the VLAN. If the masking function is enabled on the port, the port will not send these packets.

### Configuration Condition

None

### Configure Port-based Traffic Flooding

Table 7620 Configuring Explicit Congestion Notification Function Of Device

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	-
Configure Port-based Traffic Flooding	<b>flood-control</b> { <b>bcast</b>   <b>unknown-mcast</b>   <b>unknown-ucast</b> }	Mandatory  By default, traffic flooding is enabled on the port.

## 76.2.10 Hardware QoS Monitoring and Maintaining

Table 76-21 Hardware QoS Monitoring and Maintaining

Command	Description
<b>show drop-mode</b> [ <b>interface</b> <i>interface-name</i> ]	Show the drop mode of the port queue
<b>show egr-action-group</b> [ <i>egr-action-group-name</i> ]	Show related configuration information of the egress action group
<b>show l2-action-group</b> [ <i>l2-action-group-name</i> ]	Show related configuration information of the L2 action group
<b>show l3-action-group</b> [ <i>l3-action-group-name</i> ]	Show related configuration information of the L3 action group
<b>show map-table</b> <i>user-name</i> [ <i>template name</i> { <b>ingress</b>   <b>egress</b> } ]	Show priority mapping template information
<b>show queue-schedule</b> [ <b>interface</b> <i>interface-name</i> ]	Show the scheduling policy of the port queue

Command	Description
<b>show rate-limit</b> [ <b>interface</b> <i>interface-name</i> ]	Show rate limit information on the port
<b>show traffic-count</b> { <b>inst-all</b>   <b>inst-global</b>   <b>inst-vlan-range</b>   <b>inst-interface-vlan-range</b>   { <b>inst-interface</b> <i>interface-name</i>   <b>inst-interface-vlan</b> <i>vlan-id</i>   <b>inst-link-aggregation</b> <i>link-aggregation-id</i>   <b>inst-vlan</b> <i>vlan-id</i> } { <b>ip-in</b>   <b>ip-out</b>   <b>ipv6-in</b>   <b>ipv6-out</b>   <b>mac-in</b>   <b>mac-out</b> }	Show counter information of the ACL applied to the specified object
<b>show traffic-meter</b> [ <i>traffic-meter-name</i> ]	Show all information of the traffic meter
<b>show traffic-shape</b> [ <b>interface</b> <i>interface-name</i> ]	Show traffic shaping information on the port and queue
<b>show vfp-action-group</b> [ <i>vfp-action-group-name</i> ]	Show related configuration information of the VFP action group
<b>show ecn</b>	Show whether the explicit congestion notification is enabled on the device

## 76.3 Typical Configuration Example of Hardware QoS

### 76.3.1 Configure Priority Mapping

#### Network Requirements

- There are two servers on the network, namely Video Server and Data Server;
- the DSCP value in the video traffic packet is 34, and the DSCP value in the data traffic packet is 38;
- You can configure the priority mapping function so that the 802.1p priority of video traffic packets is 5 and that of data traffic packets is 1.

#### Network Topology

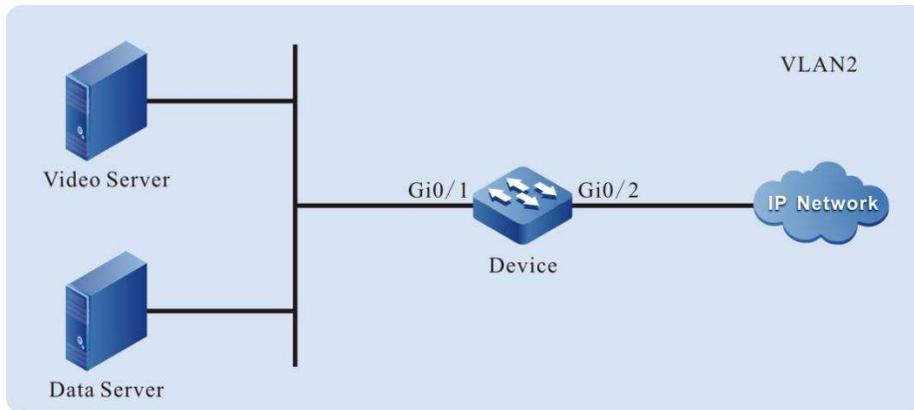


Figure 76-3 Network Topology for Configuring Priority Mapping

### Configuration Steps

*Step*  
*1:*

Configure VLAN and port link type on Device.

#Create VLAN 2.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the link type of port gigabitethernet0/1 as Access to allow services of VLAN 2 to pass.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode access
Device(config-if-gigabitethernet0/1)#switchport access vlan 2
```

#Configure the link type of port gigabitethernet0/2 to Trunk to allow services of VLAN 2 to pass.

```
Device(config-if-gigabitethernet0/1)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode trunk
Device(config-if-gigabitethernet0/2)#switchport trunk allowed vlan add 2
Device(config-if-gigabitethernet0/2)#exit
```

*Step*  
*2:*

Configure the priority mapping function.

#Configure the priority mapping function globally to map packets with DSCP value 34 to queue 2 and packets with DSCP value 38 to queue 3.

```
Device(config)#qos map-table ingress a
```

```
Device(config-mactable-ingress)#dscp-lp 34 to 2
Device(config-if-gigabitethernet0/1)# dscp-lp 38 to 3
```

#Configure the priority mapping function globally to map 802.1p priority of packets in the queue 2 as 5 and that of packets in the queue 3 as 1.

```
Device(config)#qos map-table egress b
Device(config-mactable-egress)#lp-dot1p 2 to 5
Device(config- mactable-egress)# lp-dot1p 3 to 1
```

#Bind the template and configure trust on the port

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)# map-table a ingress
Device(config-if-gigabitethernet0/1)#qos map-table trust dscp ingress
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)# map-table b egress
```

```
Device(config-if-gigabitethernet0/2)#qos map-table trust dot1p egress
```

*Step*  
3:

Check the result.

#After video traffic and data traffic are processed by Device, the 802.1p priority of the video traffic packets sent from port gigabitethernet0/2 are 5 and the 802.1p priority of the data traffic packets are 1.

## 76.3.2 Configure Remarking

### Network Requirements

- There are two servers on the network, namely Video Server and Data Server;
- You can configure the remarking function so that the 802.1p priority of video traffic packets can be marked as 5 and that of data traffic packets remains unchanged.

### Network Topology

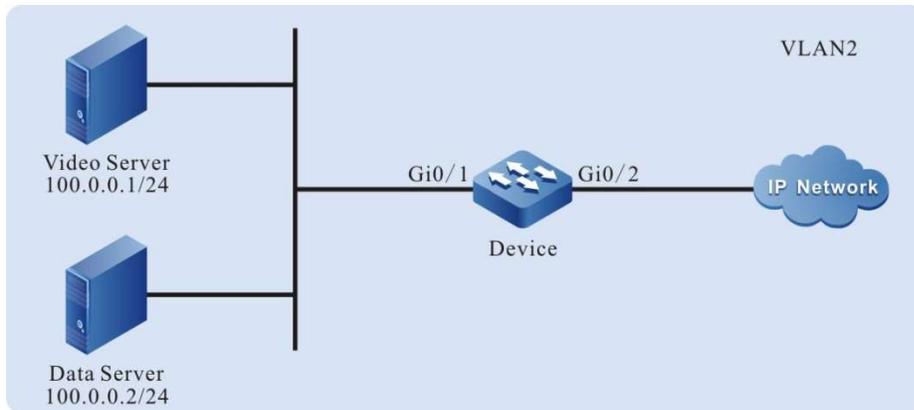


Figure 76-4 Network Topology for Configuring Remarking

### Configuration Steps

*Step 1:* Configure VLAN and port link type on Device.

#Create VLAN 2.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the link type of port gigabitethernet0/1 as Access to allow services of VLAN 2 to pass.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode access
Device(config-if-gigabitethernet0/1)#switchport access vlan 2
```

#Configure the link type of port gigabitethernet0/2 to Trunk to allow services of VLAN 2 to pass.

```
Device(config-if-gigabitethernet0/1)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode trunk
Device(config-if-gigabitethernet0/2)#switchport trunk allowed vlan add 2
Device(config-if-gigabitethernet0/2)#exit
```

*Step 2:* Configure the L3 action group.

#Configure the L3 action group named remark. The action is to remark the 802.1p priority of the packets to 5.

```
Device(config)#l3-action-group remark
Device(config-action-group)#remark l2-priority dot1p 5
Device(config-action-group)#exit
```

*Step*  
3:

Configure the standard IP ACL.

#Configure the standard IP ACL numbered 1 on Device.

```
Device(config)#ip access-list standard 1
```

#Configure binding of rules to the L3 action group named remark so that the 802.1p priority of the video traffic packets can be remarked as 5.

```
Device(config-std-nacl)#permit host 100.0.0.1 l3-action-group remark
```

#Configure rules to allow data traffic to pass without changing the 802.1p priority of packets.

```
Device(config-std-nacl)#permit host 100.0.0.2
```

```
Device(config-std-nacl)#commit
```

```
Device(config-std-nacl)#exit
```

*Step*  
4:

Configure applying of the standard IP ACL.

#Apply the standard IP ACL numbered 1 to the ingress direction of port gigabitethernet0/1 of Device.

```
Device(config)#interface gigabitethernet 0/1
```

```
Device(config-if-gigabitethernet0/1)#ip access-group 1 in
```

```
Device(config-if-gigabitethernet0/1)#exit
```

#View on Device, the information of the ACL applied to the port.

```
Device#show acl-object interface
```

```
-----Interface----Bind----Instance-----
```

```
Interface-----Direction----AclType----AclName
```

```
gi0/1          IN      IP      1
```

*Step*  
5:

Check the result.

#After video traffic and data traffic are processed by Device, the 802.1p priority of the video traffic packets sent from port gigabitethernet0/2 is modified into 5, and that of the data traffic packets remains unchanged.

### 76.3.3 Configure Traffic Shaping

#### Network Requirements

- There are two servers on the network, namely Video Server and Data Server;
- Configure the traffic shaping function to ensure that the video traffic rate is 20,000 kbps but the maximum is less than 20,000 kbps, and the sum of the video traffic rate and data traffic rate does not exceed 50,000 kbps. If the video traffic rate is greater than 20,000 kbps, you need to limit the video traffic rate to 20,000 kbps. If the video traffic rate is less than 20,000 kbps, the remaining bandwidth can be occupied by data traffic.

#### Network Topology

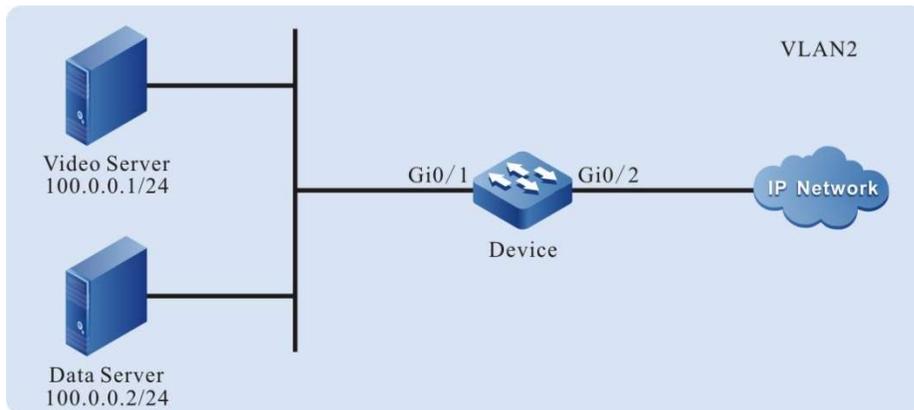


Figure 76-5 Network Topology for Configuring Traffic Shaping

#### Configuration Steps

*Step 1:* Configure VLAN and port link type on Device.

#Create VLAN 2.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

**#Configure the link type of port gigabitethernet0/1 as Access to allow services of VLAN 2 to pass.**

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode access
Device(config-if-gigabitethernet0/1)#switchport access vlan 2
```

**#Configure the link type of port gigabitethernet0/2 to Trunk to allow services of VLAN 2 to pass.**

```
Device(config-if-gigabitethernet0/1)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode trunk
Device(config-if-gigabitethernet0/2)#switchport trunk allowed vlan add 2
Device(config-if-gigabitethernet0/2)#exit
```

*Step*  
*2:*

**Configure the L3 action group.**

**#Configure the L3 action group named LP7. The action is to remark the packets to queue 7.**

```
Device(config)#l3-action-group LP7
Device(config-action-group)#remark l2-priority 1p 7
Device(config-action-group)#exit
```

**#Configure the L3 action group named LP6. The action is to remark the packets to queue 6.**

```
Device(config)#l3-action-group LP6
Device(config-action-group)#remark l2-priority 1p 6
Device(config-action-group)#exit
```

*Step*  
*3:*

**Configure the standard IP ACL.**

**#Configure the standard IP ACL numbered 1 on Device.**

```
Device(config)#ip access-list standard 1
```

**#Configure binding of rules to the L3 action group named LP7 so that the video traffic packets can be remarked to the queue 7.**

```
Device(config-std-nacl)#permit host 100.0.0.1 l3-action-group LP7
```

**#Configure binding of rules to the L3 action group named LP6 so that the data traffic packets can be remarked to the queue 6.**

```
Device(config-std-nacl)#permit host 100.0.0.2 13-action-group LP6
Device(config-std-nacl)#commit
Device(config-std-nacl)#exit
```

*Step*  
4:

Configure applying of the standard IP ACL.

#Apply the standard IP ACL numbered 1 to the ingress direction of port gigabitethernet0/1 of Device.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#ip access-group 1 in
Device(config-if-gigabitethernet0/1)#exit
```

#View on Device, the information of the ACL applied to the port.

```
Device#show acl-object interface
-----Interface-----Bind----Instance-----
Interface-----Direction----AclType----AclName
gi0/1             IN      IP      1
```

*Step*  
5:

Configure the traffic shaping function.

#Configure queue-based traffic shaping on port gigabitethernet0/2. The traffic rate of the queue 7 is limited to 20000 kbps.

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#traffic-shape queue 7 cir 20000 pir 20000
```

#Configure queue-based traffic shaping on port gigabitethernet0/2. The traffic rate of the whole port is limited to 50000 kbps.

```
Device(config-if-gigabitethernet0/2)#traffic-shape pir 50000
Device(config-if-gigabitethernet0/2)#exit
```

*Step*  
6:

Check the result.

#After video traffic and data traffic are processed by Device, the sum of the video traffic rate and data traffic rate from port gigabitethernet0/2 does not exceed 50000 kbps. If the video traffic rate is greater than 20,000 KBPS, limit the video

traffic rate to 20000 kbps. If the video traffic rate is less than 20000 kbps, the remaining bandwidth can be occupied by data traffic.

### 76.3.4 Configure Rate Limiting

#### Network Requirements

- There are two servers on the network, namely Video Server and Data Server;
- Configure the rate limiting function to limit the sum of the video traffic rate and data traffic rate to not exceed 50000 kbps with the data traffic rate not exceeding 20000 kbps.

#### Network Topology

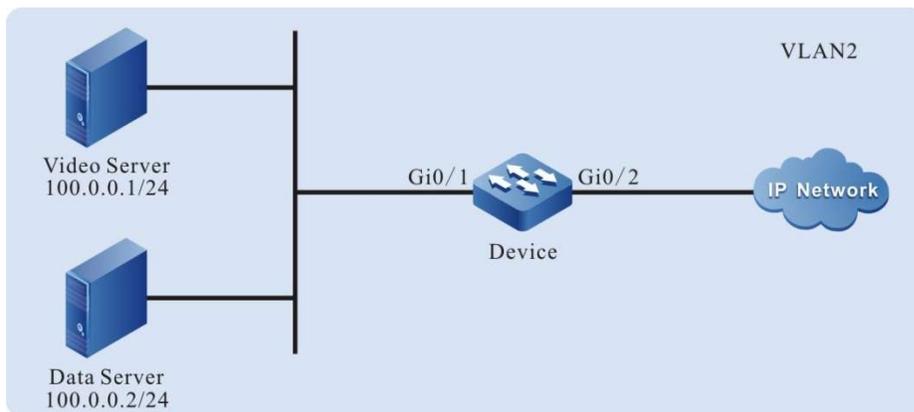


Figure 76-6 Network Topology for Configuring Rate Limiting

#### Configuration Steps

*Step 1:* Configure VLAN and port link type on Device.

#Create VLAN 2.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the link type of port gigabitethernet0/1 as Access to allow services of VLAN 2 to pass.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode access
Device(config-if-gigabitethernet0/1)#switchport access vlan 2
```

#Configure the link type of port gigabitethernet0/2 to Trunk to allow services of VLAN 2 to pass.

```
Device(config-if-gigabitethernet0/1)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode trunk
Device(config-if-gigabitethernet0/2)#switchport trunk allowed vlan add 2
Device(config-if-gigabitethernet0/2)#exit
```

*Step*  
2:

Configure the rate limiting function.

#Configure queue-based traffic limiting on port gigabitethernet0/1. The traffic rate is limited to 50000 kbps.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#rate-limit default 50000 4096
Device(config-if-gigabitethernet0/1)#exit
```

*Step*  
3:

Configure the meter function.

#Configure the traffic meter named data\_stream. The traffic rate is limited to 20000 kbps.

```
Device(config)#traffic-meter data_stream
Device(config-meter)#meter mode srtcm 20000 4096 4096
Device(config-meter)#exit
```

*Step*  
4:

Configure the egress action group.

#Configure the egress action group named data\_stream, and apply the traffic meter in the egress action group.

```
Device(config)#egr-action-group data_stream
Device(config-egract-group)#meter data_stream
Device(config-egract-group)#exit
```

*Step*  
5:

Configure the standard IP ACL.

#Configure the standard IP ACL numbered 1 on Device.

```
Device(config)#ip access-list standard 1
```

#Configure binding of rules to the egress action group named data\_stream. The data rate is limited to 20000 kbps.

```
Device(config-std-nacl)#permit host 100.0.0.2 egr-action-group data_stream
```

#Configure rules to allow video traffic to pass.

```
Device(config-std-nacl)#permit host 100.0.0.1
```

```
Device(config-std-nacl)#commit
```

```
Device(config-std-nacl)#exit
```

*Step*  
*6:*

Configure applying of the standard IP ACL.

#Apply the standard IP ACL numbered 1 to the egress direction of port gigabitethernet0/2 of Device.

```
Device(config)#interface gigabitethernet 0/2
```

```
Device(config-if-gigabitethernet0/2)#ip access-group 1 out
```

```
Device(config-if-gigabitethernet0/2)#exit
```

#View on Device, the information of the ACL applied to the port.

```
Device#show acl-object interface
```

```
-----Interface-----Bind----Instance-----
```

```
Interface-----Direction----AclType----AclName
```

```
gi0/2          OUT      IP      1
```

*Step*  
*7:*

Check the result.

#After video traffic and data traffic are processed by Device, the sum of the video traffic rate and data traffic rate from port gigabitethernet0/2 does not exceed 50000 kbps with the data traffic rate not exceeding 20000 kbps.

## 76.3.5 Configure WRED

### Network Requirements

- Numerous terminals download files from the FTP server.
- Configure the WRED function on Device to prevent the global synchronization of TCP from causing intermittent FTP connections.

## Network Topology

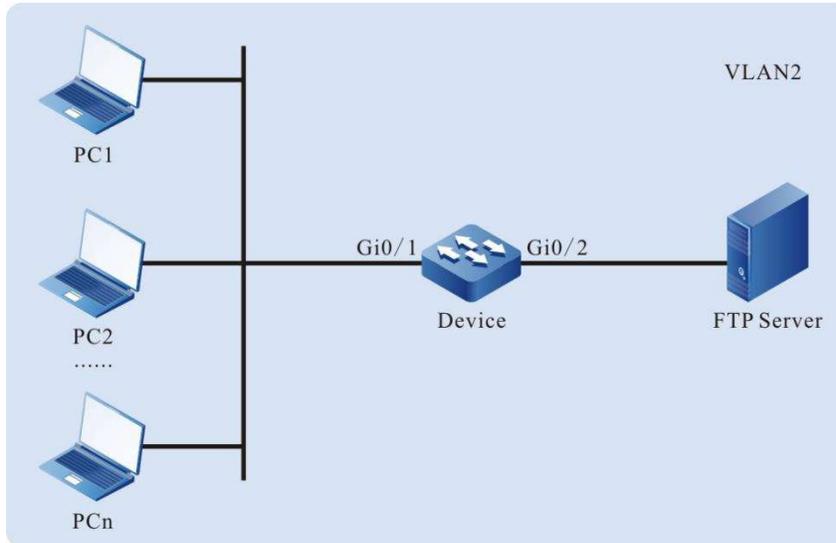


Figure 76-7 Network Topology for Configuring WRED

## Configuration Steps

*Step 1:*

Configure VLAN and port link type on Device.

#Create VLAN 2.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the link type of port gigabitethernet0/1 as Access to allow services of VLAN 2 to pass.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode access
Device(config-if-gigabitethernet0/1)#switchport access vlan 2
```

#Configure the link type of port gigabitethernet0/2 to Trunk to allow services of VLAN 2 to pass.

```
Device(config-if-gigabitethernet0/1)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode trunk
Device(config-if-gigabitethernet0/2)#switchport trunk allowed vlan add 2
```

```
Device(config-if-gigabitethernet0/2)#exit
```

*Step*  
*2:*

Configure the WRED function.

#Configure the drop-start value of queue 0 packets on port gigabitethernet0/2 to 80, with drop rate of 45.

```
Device(config)#interface gigabitethernet 0/2
```

```
Device(config-if-gigabitethernet0/2)#drop-mode 0 wred drop-start 80 drop-rate 45
```

```
Device(config-if-gigabitethernet0/2)#exit
```

---

### Note

- The packets sent by PC are all Untag packets and enter the queue 0 by default.
- 

*Step*  
*3:*

Check the result.

#When numerous terminals download files from the FTP server, there will be no intermittent connection to FTP.

## 76.3.6 Configure SP

### Network Requirements

- There are authentication server (AAA Server), video server (Video Server) and one terminal device (PC) on the network;
- Configure the SP function to guarantee, when egress port traffic is congested, the traffic of the authentication server first, the video traffic second, and the terminal traffic last.

### Network Topology

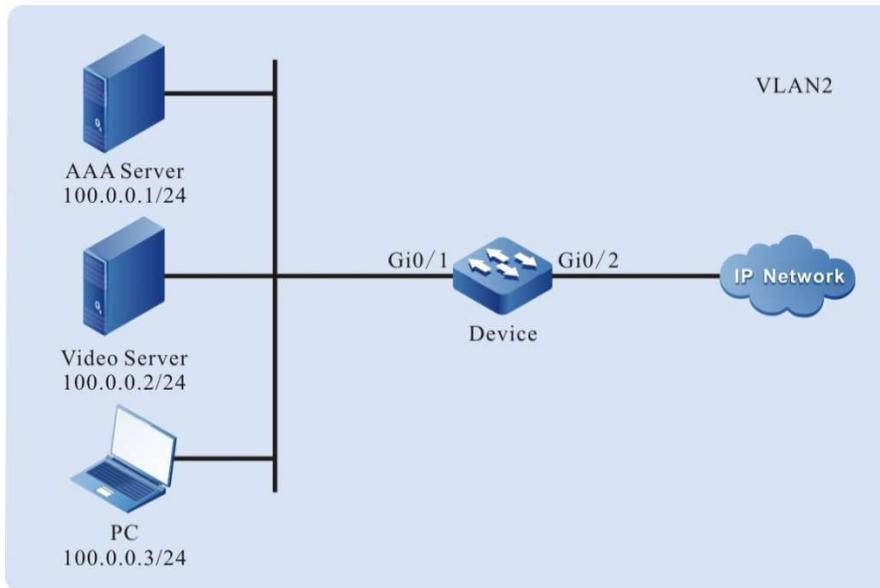


Figure 76-8 Network Topology for Configuring SP

### Configuration Steps

*Step 1:* Configure VLAN and port link type on Device.

#Create VLAN 2.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the link type of port gigabitethernet0/1 as Access to allow services of VLAN 2 to pass.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode access
Device(config-if-gigabitethernet0/1)#switchport access vlan 2
```

#Configure the link type of port gigabitethernet0/2 to Trunk to allow services of VLAN 2 to pass.

```
Device(config-if-gigabitethernet0/1)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode trunk
Device(config-if-gigabitethernet0/2)#switchport trunk allowed vlan add 2
Device(config-if-gigabitethernet0/2)#exit
```

*Step*  
2:

Configure the L3 action group.

#Configure the L3 action group named LP7. The action is to remark the packets to queue 7.

```
Device(config)#l3-action-group LP7
Device(config-action-group)#remark l2-priority 1p 7
Device(config-action-group)#exit
```

#Configure the L3 action group named LP6. The action is to remark the packets to queue 6.

```
Device(config)#l3-action-group LP6
Device(config-action-group)#remark l2-priority 1p 6
Device(config-action-group)#exit
```

#Configure the L3 action group named LP5. The action is to remark the packets to queue 5.

```
Device(config)#l3-action-group LP5
Device(config-action-group)#remark l2-priority 1p 5
Device(config-action-group)#exit
```

*Step*  
3:

Configure the standard IP ACL.

#Configure the standard IP ACL numbered 1 on Device.

```
Device(config)#ip access-list standard 1
```

#Configure binding of rules to the L3 action group named LP7 so that the authentication traffic packets can be remarked to the queue 7.

```
Device(config-std-nacl)#permit host 100.0.0.1 l3-action-group LP7
```

#Configure binding of rules to the L3 action group named LP6 so that the video traffic packets can be remarked to the queue 6.

```
Device(config-std-nacl)#permit host 100.0.0.2 l3-action-group LP6
```

#Configure binding of rules to the L3 action group named LP5 so that the terminal traffic packets can be remarked to the queue 5.

```
Device(config-std-nacl)#permit host 100.0.0.3 l3-action-group LP5
Device(config-std-nacl)#commit
Device(config-std-nacl)#exit
```

Step  
4:

Configure applying of the standard IP ACL.

#Apply the standard IP ACL numbered 1 to the ingress direction of port gigabitethernet0/1 of Device.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#ip access-group 1 in
Device(config-if-gigabitethernet0/1)#exit
```

#View on Device, the information of the ACL applied to the port.

```
Device#show acl-object interface
-----Interface-----Bind----Instance-----
Interface-----Direction---AclType---AclName
gi0/1             IN      IP      1
```

Step  
5:

Configure the SP function.

#Configure the SP function on port gigabitethernet0/2 to perform strict priority scheduling on packets.

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#queue-schedule sp
Device(config-if-gigabitethernet0/2)#exit
```

Step  
6:

Check the result.

#When the traffic of the egress port gigabitethernet0/2 is congested, the authentication traffic is given priority to pass, the video traffic is then allowed to pass, and finally the terminal traffic is allowed to pass.

## 76.3.7 Configure WDRR

### Network Requirements

- There are authentication server (AAA Server), video server (Video Server) and one terminal device (PC) on the network;
- Configure the WDRR function to enable terminal traffic, video traffic, and

authentication traffic to pass in a specific ratio when the egress port traffic is congested.

## Network Topology

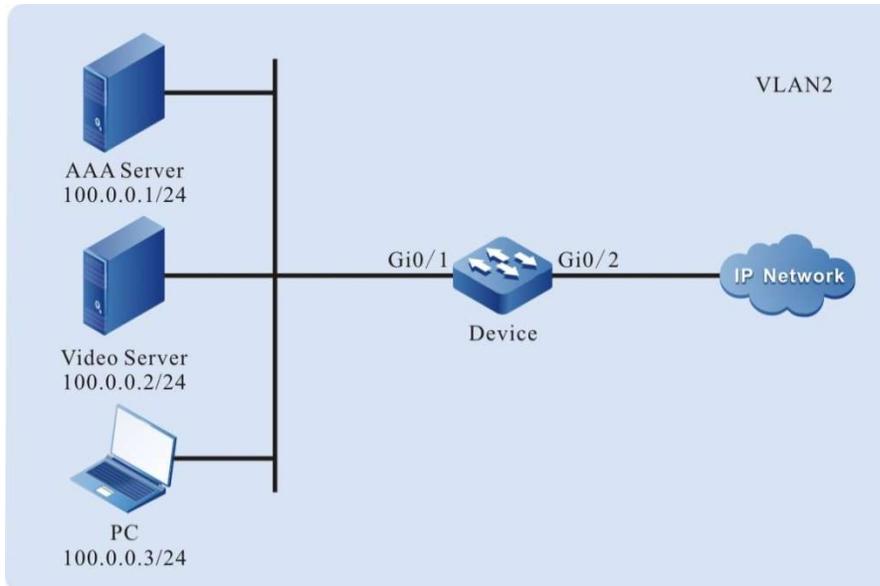


Figure 76-9 Network Topology for Configuring WDRR

## Configuration Steps

*Step 1:*

Configure VLAN and port link type on Device.

#Create VLAN 2.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the link type of port gigabitethernet0/1 as Access to allow services of VLAN 2 to pass.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode access
Device(config-if-gigabitethernet0/1)#switchport access vlan 2
```

#Configure the link type of port gigabitethernet0/2 to Trunk to allow services of VLAN 2 to pass.

```
Device(config-if-gigabitethernet0/1)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode trunk
Device(config-if-gigabitethernet0/2)#switchport trunk allowed vlan add 2
Device(config-if-gigabitethernet0/2)#exit
```

*Step*  
2:

Configure the L3 action group.

#Configure the L3 action group named LP7. The action is to remark the packets to queue 7.

```
Device(config)#l3-action-group LP7
Device(config-action-group)#remark l2-priority 1p 7
Device(config-action-group)#exit
```

#Configure the L3 action group named LP6. The action is to remark the packets to queue 6.

```
Device(config)#l3-action-group LP6
Device(config-action-group)#remark l2-priority 1p 6
Device(config-action-group)#exit
```

#Configure the L3 action group named LP5. The action is to remark the packets to queue 5.

```
Device(config)#l3-action-group LP5
Device(config-action-group)#remark l2-priority 1p 5
Device(config-action-group)#exit
```

*Step*  
3:

Configure the standard IP ACL.

#Configure the standard IP ACL numbered 1 on Device.

```
Device(config)#ip access-list standard 1
```

#Configure binding of rules to the L3 action group named LP7 so that the authentication traffic packets can be remarked to the queue 7.

```
Device(config-std-nacl)#permit host 100.0.0.1 l3-action-group LP7
```

#Configure binding of rules to the L3 action group named LP6 so that the video traffic packets can be remarked to the queue 6.

```
Device(config-std-nacl)#permit host 100.0.0.2 l3-action-group LP6
```

#Configure binding of rules to the L3 action group named LP5 so that the terminal traffic packets can be remarked to the queue 5.

```
Device(config-std-nacl)#permit host 100.0.0.3 l3-action-group LP5
Device(config-std-nacl)#commit
Device(config-std-nacl)#exit
```

*Step*  
4:

Configure applying of the standard IP ACL.

#Apply the standard IP ACL numbered 1 to the ingress direction of port gigabitethernet0/1 of Device.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#ip access-group 1 in
Device(config-if-gigabitethernet0/1)#exit
```

#View on Device, the information of the ACL applied to the port.

```
Device#show acl-object interface
-----Interface-----Bind----Instance-----
Interface-----Direction----AclType----AclName
gi0/1             IN      IP      1
```

*Step*  
5:

Configure the WDRR function.

#Configure the WDRR function on port gigabitethernet0/2 to schedule respectively the packets in queues 5, 6, and 7 according to the ratio of 1:2:3.

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#queue-schedule wdr 1 1 1 1 1 2 3
Device(config-if-gigabitethernet0/2)#exit
```

*Step*  
6:

Check the result.

#Terminal traffic, video traffic, and authentication traffic can pass in the specific ratio of 1:2:3 when the traffic of the egress port gigabitethernet0/2 is congested.

## 76.3.8 Configure SP+WDRR

### Network Requirements

- There are authentication server (AAA Server), video server (Video Server) and one terminal device (PC) on the network.

- Configure the SP+WDRR function to guarantee that when the traffic of the egress port is congested, all the traffic of the authentication server is given priority to pass, and the terminal traffic and video traffic can pass according to the ratio of 1:2.

## Network Topology

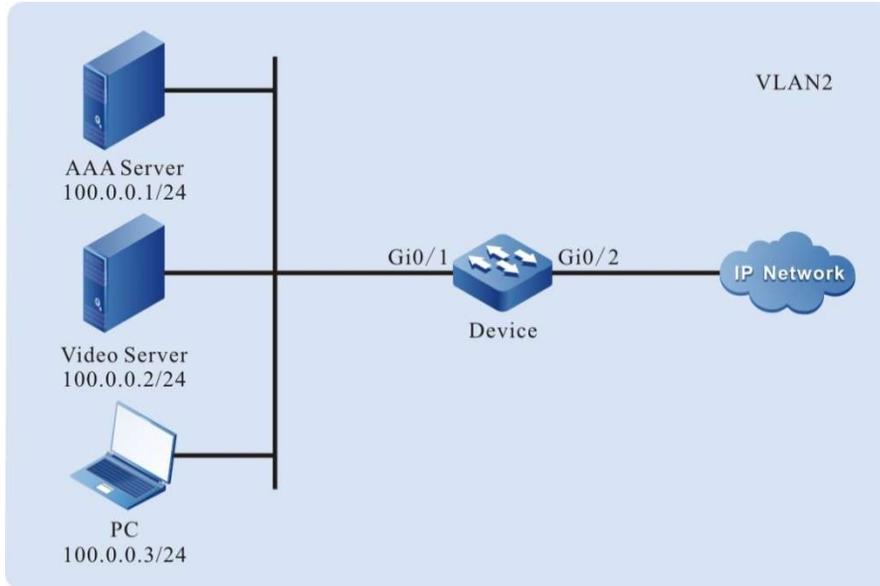


Figure 76-10 Network Topology for Configuring SP+WDRR

## Configuration Steps

*Step 1:*

Configure VLAN and port link type on Device.

#Create VLAN 2.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the link type of port gigabitethernet0/1 as Access to allow services of VLAN 2 to pass.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode access
Device(config-if-gigabitethernet0/1)#switchport access vlan 2
```

#Configure the link type of port gigabitethernet0/2 to Trunk to allow services of VLAN 2 to pass.

```
Device(config-if-gigabitethernet0/1)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode trunk
```

```
Device(config-if-gigabitethernet0/2)#switchport trunk allowed vlan add 2
Device(config-if-gigabitethernet0/2)#exit
```

*Step*  
*2:*

Configure the L3 action group.

#Configure the L3 action group named LP7. The action is to remark the packets to queue 7.

```
Device(config)#l3-action-group LP7
Device(config-action-group)#remark l2-priority 1p 7
Device(config-action-group)#exit
```

#Configure the L3 action group named LP6. The action is to remark the packets to queue 6.

```
Device(config)#l3-action-group LP6
Device(config-action-group)#remark l2-priority 1p 6
Device(config-action-group)#exit
```

#Configure the L3 action group named LP5. The action is to remark the packets to queue 5.

```
Device(config)#l3-action-group LP5
Device(config-action-group)#remark l2-priority 1p 5
Device(config-action-group)#exit
```

*Step*  
*3:*

Configure the standard IP ACL.

#Configure the standard IP ACL numbered 1 on Device.

```
Device(config)#ip access-list standard 1
```

#Configure binding of rules to the L3 action group named LP7 so that the authentication traffic packets can be remarked to the queue 7.

```
Device(config-std-nacl)#permit host 100.0.0.1 l3-action-group LP7
```

#Configure binding of rules to the L3 action group named LP6 so that the video traffic packets can be remarked to the queue 6.

```
Device(config-std-nacl)#permit host 100.0.0.2 l3-action-group LP6
```

#Configure binding of rules to the L3 action group named LP5 so that the terminal traffic packets can be remarked to the queue 5.

```
Device(config-std-nacl)#permit host 100.0.0.3 l3-action-group LP5
```

```
Device(config-std-nacl)#commit
Device(config-std-nacl)#exit
```

*Step*  
4:

Configure applying of the standard IP ACL.

#Apply the standard IP ACL numbered 1 to the ingress direction of port gigabitethernet0/1 of Device.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#ip access-group 1 in
Device(config-if-gigabitethernet0/1)#exit
```

#View on Device, the information of the ACL applied to the port.

```
Device#show acl-object interface
-----Interface-----Bind-----Instance-----
Interface-----Direction---AcIType---AcIName
gi0/1             IN      IP      1
```

*Step*  
5:

Configure the SP+WDRR function.

#Configure the SP+WDRR function on port gigabitethernet0/2 to allow all the packets in the queue 7 to pass. The packets in the queue 5 and queue 6 are scheduled according to the ratio of 1:2.

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#queue-schedule wdr 1 1 1 1 1 2 0
Device(config-if-gigabitethernet0/2)#exit
```

*Step*  
6:

Check the result.

#All the authentication traffic is given priority to pass when the traffic of the egress port gigabitethernet0/2 is congested. The terminal traffic and the video traffic pass in the ratio of 1:2.

## 76.3.9 Configure Flow Mirror

### Network Requirements

- PC 1, PC 2, and PC 3 are connected to Device, and PC 1 and PC 2 communicate in VLAN 2;
- Configure the flow mirror function on Device, so that PC 3 monitors packets received by Device port gigabitethernet0/1.

### Network Topology

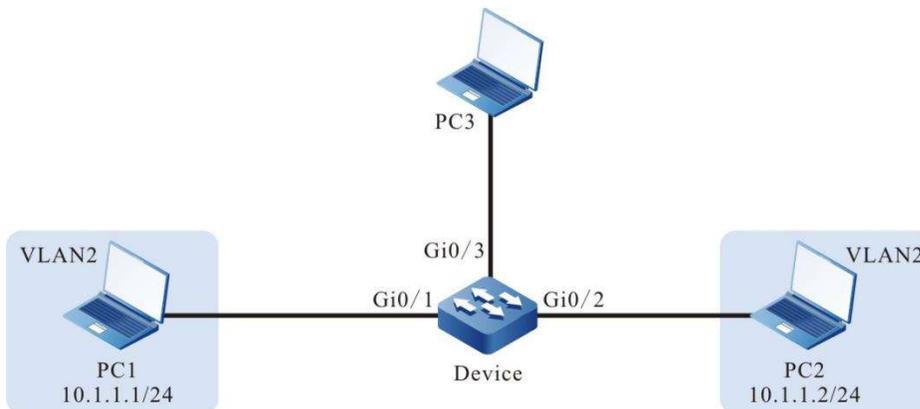


Figure 76-11 Network Topology for Configuring Flow Mirror

### Configuration Steps

*S*  
*t*  
*e*  
*p*  
*l*  
*:*

Configure VLANs and the link type of the ports.

# Create VLAN2 on Device.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the link type of ports gigabitethernet0/1 and gigabitethernet0/2 on Device as Access, allowing the services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/1-0/2
Device(config-if-range)#switchport mode access
Device(config-if-range)#switchport access vlan 2
Device(config-if-range)#exit
```

*S*  
*t*  
*e*  
*p*  
*2*  
*:*

Configure the flow mirror function.

#Configure the L3 action group named mirror to mirror the packets to port gigabitethernet0/3.

```
Device(config)#l3-action-group mirror
Device(config-action-group)#mirror interface gigabitethernet 0/3
Device(config-action-group)#exit
```

*S*  
*t*  
*e*  
*p*  
*3*  
*:*

Configure the standard ACL.

#Configure the standard IP ACL numbered 1 on Device.

```
Device(config)#ip access-list standard 1
```

#Configure binding of rules to the L3 action group named mirror so that all the packets can be mirrored to the port gigabitethernet0/3.

```
Device(config-std-nacl)#permit any l3-action-group mirror
Device(config-std-nacl)#commit
Device(config-std-nacl)#exit
```

*S*  
*t*  
*e*  
*p*  
*4*  
*:*

Configure applying of the standard IP ACL.

#Apply the standard IP ACL numbered 1 to the ingress direction of port gigabitethernet0/1 of Device.

```
Device(config)#interface gigabitethernet 0/1
```

```
Device(config-if-gigabitethernet0/1)#ip access-group 1 in
Device(config-if-gigabitethernet0/1)#exit
```

*S*  
*t*  
*e*  
*p*  
*5*  
*:*

Check the result.

#When PC 1 and PC 2 communicate with each other, the packets received on port gigabitethernet0/1 can be captured on PC 3.

# 77 MPLS Basics

---

## 77.1 Overview

MPLS (Multiprotocol Label Switching) integrates the simplicity of Layer 2 switching with the flexibility of Layer 3 routing to provide connection-oriented features for connectionless IP networks.

MPLS has the following technical advantages over traditional IP network technologies:

- Label-based group forwarding simplifies the forwarding mechanism and improves forwarding efficiency.
- By introducing labels, service functions can be flexibly extended to achieve routing,

traffic engineering, QoS, VPN, and other functions.

- The labels themselves have no specific meaning and can map the target IP addresses, fiber channels, wavelengths or even VC channels in SDH/SONET, etc.

The following is an introduction to some important basic concepts of MPLS.

### 1. Forwarding Equivalence Class (FEC)

Forwarding Equivalence Class (FEC) refers to the set of packets that follow the same forwarding path in the network (the destination address of the packets can be different), and the packets with the same FEC are processed in the same way by the LSR during the forwarding process. The ingress LSR of the MPLS network finds the corresponding label value for IP packets entering the MPLS domain according to the FEC and encapsulates it in the packet to form a label packet, which is transmitted in the MPLS network.

### 2. Label

In an MPLS network, MPLS packets are forwarded according to the label carried by the packet, which is inserted between the headers of Layer 3 and Layer 2 and is called the MPLS label header, whose format is shown in Figure 1.

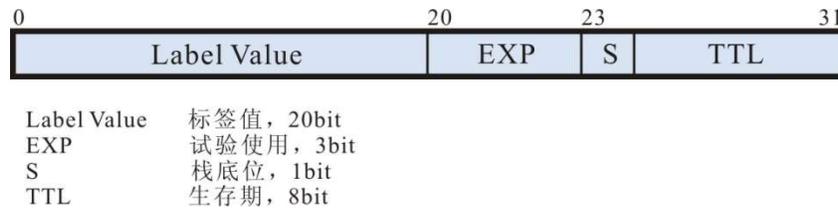


Figure 77-1 MPLS Label Structure

An MPLS packet can also carry multiple label headers in a structure called a label stack, which is organized in a "last-in, first-out" manner, with the outermost label called the top-of-stack label and the innermost label called the bottom-of-stack label, each label consisting of the following fields,

- Time to live (TTL): 8-bit, having the same function as the TTL field in the IP header.
- Bottom-of-stack (S): 1-bit, a value of 1 indicates that the corresponding label is the last label in the label stack (bottom of the stack); 0-bit indicates all other labels except for the bottom-of-stack label.
- Experimental (EXP): 3-bit, reserved, not specified in the protocol, usually used to specify Classes of Services.
- Label Value: 20-bit, used to identify the FEC. Labels 0 through 15 are reserved labels. The specific meaning of each label value is as follows.

Table 77-1 Meaning of Reserved Label Value

Label value	Meaning
-------------	---------

0	IPv4 Explicit Null label
1	Router Alert label
2	IPv6 Explicit Null label
3	Implicit Null label
4 - 15	Suspended

### 3. Label Switching Router

LSR (Label Switching Router) is a device that supports MPLS services, distributes labels, and receives and transmits packets with labels over the data link.

### 4. Label Edge Router

LER (Label Edge Router) is an LSR that is at the edge of the MPLS network and connects to other networks.

### 5. Label Switched Path

LSP (Label Switched Path) is the forwarding path of packets with the same FEC in the MPLS network.

### 6. MPLS Network Node

The MPLS network includes the following important network nodes:

- **Ingress node:** The ingress LER of the MPLS network, which encapsulates the label for the packets entering the MPLS network.
- **Transit node:** An LSR inside the MPLS network that looks up the MPLS forwarding table based on the label and performs labeling operations to send the packet along the LSP to the egress LER.
- **Egress node:** The egress LER of the MPLS network, responsible for removing the label and sending the packet to the destination network.

### 7. Label Forwarding Table

LFIB (Label Forwarding Information Base), similar to the IP FIB, is used to forward MPLS packets. It includes the following types:

- **NHLFE** (Next Hop Label Forwarding Entry): Records the MPLS forwarding operation method and forwarding information.
- **FTN** (FEC to NHLFE, FEC mapping to NHLFE): Used to look up FTN at Ingress node based on the FEC of the packet to be mapped to the NHLFE table entry.
- **ILM** (Incoming Label Map): Used to look up ILM based on incoming labels to be mapped to the NHLFE table entry.

## 77.2 MPLS Basic Function Configuration

Table 77-2 MPLS Basic Function Configuration List

Configuration Task	
Configure basic functions of MPLS.	Enable global MPLS function
	Enable interface MPLS function
	Configure label assignment ranges.
Configure MPLS forwarding control.	Configure packet load templates.
	Configure packet TTL replication method.
	Configure packet TTL timeout handling method.

### 77.2.1 Configure basic functions of MPLS.

On routers involved in MPLS forwarding, you need to enable the MPLS function globally and on the interface.

#### Configuration Condition

Before configuring the basic functions of MPLS, do the following:

- The link layer protocol has been configured to ensure normal communication at the link layer.
- Configure address of interface at network layer so that neighbor network nodes are reachable at the network layer.
- Configure static routes or IGP protocols to ensure that each LSR can communicate at the network layer.

#### Enable global MPLS function

Table 77-3 Enabling Global MPLS Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Enable global MPLS function	<b>mpls ip</b>	Mandatory By default, the MPLS function is not enabled.

### Enable interface MPLS function

Table 77-4 Enabling Interface MPLS Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface_name</i>	-
Enable interface MPLS function	<b>mpls ip</b>	Mandatory By default, the interface MPLS function is not enabled.

### Configure label assignment ranges.

Table 77-5 Configuring Label Assignment Ranges

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the range of locally assigned label.	<b>mpls label range</b> <i>min-label max-label</i>	Optional By default, the allowed range for label value assignment is 16~1048575.

---

## Caution

- Generally, you do not need to configure the range of locally distributed labels. If you configure this function after configuring the protocol for allocating label resources (such as LDP, BGP), you need to save and reboot the device to take effect.
- 

### 77.2.2 Configure MPLS forwarding control.

#### Configuration Condition

Before configuring MPLS forwarding control, do the following:

- Enable MPLS basic functions globally and on the interface to ensure that MPLS packets can be sent and received.

#### Configure packet load templates.

In the MPLS network, you can set up multipath packet load templates with a command.

Table 77-6 Configuring Packet Load Templates

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure MPLS packet load method.	<b>mpls load-balancing profile</b> <i>profile-name</i>	Optional By default, the default template is used.

#### Configure packet TTL replication method.

At the Ingress node of the MPLS network, when IP packets are encapsulated with a label, the system by default copies the TTL value of the IP packet minus one into the TTL field of the MPLS label. Users can also set the TTL field of the MPLS label to 255 through a configuration command to stop copying the TTL value of IP packets.

Table 77-7 Configuring Packet TTL Replication Method

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the MPLS packet TTL replication method to not replicate the TTL value in IP packets.	<b>no mpls ttl-propagate</b> [ <b>forwarded</b>   <b>local</b> ]	Optional By default, forwarded packets and locally sent packets copy the TTL value of the IP packet minus one into the TTL field of the MPLS label.

### Configure packet TTL timeout handling method.

When the LSR receives an MPLS packet with a TTL of 1, the LSR generates a TTL-expired ICMP packet. The LSR returns the ICMP packet to the sender of the packet in one of two ways:

- Forwarding ICMP packets along the original LSP, finding the route to the packet sender at the Egress node, and returning the ICMP packet to the packet sender.
- The route to the sender of the packet is queried on the LSR device where the TTL timeout is found, and the ICMP packet is returned to the sender of the packet.

The **mpls ttl-expiration** command allows you to configure the number of label layers. When the TTL timeout of an MPLS packet is found, the number of incoming label layers is compared with the configured number of label layers to determine how ICMP packets should be sent. If the number of incoming label layers does not exceed the configured number of label layers, the second method will be used to return ICMP packets to the sender, and the first method will be used vice versa.

Table 77-8 Configuring Packet TTL Timeout Handling Method

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the number of label layers for packet TTL timeout handling.	<b>mpls ttl-expiration</b> <i>labels-num</i>	Optional By default, the number of label layers for packet TTL timeout handling is 1.

### 77.2.3 MPLS Basic Monitoring and Maintaining

Table 77-9 MPLS Basic Monitoring and Maintaining

Command	Description
<b>clear mpls forwarding-table statistics</b>	Clear the packet count statistics of the MPLS service.
<b>show mpls forwarding-table</b> [ detail ]	Display MPLS forwarding table information.
<b>show mpls forwarding-table ilm</b> [ <i>A.B.C.D</i> [ <i>mask</i> ] ]   <b>in-label</b> <i>in-label</i>   <b>ipv4</b>   <b>sr</b>   <b>mcast</b> [ <i>in-label</i> ]   <b>vrf</b> <i>vrf-name</i> ] [ <b>detail</b> ]	Display MPLS ILM forwarding table information.
<b>show mpls forwarding-table statistics</b> { <b>packet</b>   <b>record</b> }	Display the statistics of MPLS forwarding packets and the number of each type of forwarding table.
<b>show mpls label range</b>	Show label assignment range.
<b>show mpls label used-block-data</b> [ <b>detail</b> ]	Display MPLS label block assignment information.

# 78 MPLS LDP

---

## 78.1 Overview

LDP (Label Distribution Protocol) is a basic signaling protocol for MPLS, which is used for label distribution and advertisement to dynamically establish LSP (Label Switching Path).

In addition to label distribution, LDP has a number of features:

- Support label filtering: Selectively advertise and receive labels through access control lists to achieve the purpose of saving resources and reducing network burden.
- Support loopback detection: Avoid LSP loops by loopback detection.
- Support MD5 authentication: Enhance the security of information interaction between LSRs.
- Support GR capability: Achieve uninterrupted data transmission when there is a failure at the device control level.
- Support BFD linkage: Fast convergence at LDP protocol level through BFD fast detection.

## 78.2 MPLS LDP Function Configuration

Table 1-2 LDP Function Configuration List

Configuration Task	
Configure basic functions of LDP.	Enable LDP Protocol.
Configure LDP neighbor parameters.	Configure parameters of directly connected session.
	Configure remote session parameters.
Configure LDP MD5 authentication.	Configure LDP MD5 authentication.

Configuration Task	
Configure LDP control attributes.	Configure label reception filtering.
	Configure label advertisement filtering.
	Configuration label re-advertisement.
	Configure label assignment control method.
	Configure PHP features.
	Configure loopback detection.
	Configure session reconnection.
Configure LDP GR.	Configure LDP GR.
Configure LDP to coordinate with BFD.	Configure LDP to coordinate with BFD.

### 78.2.1 Configure basic functions of LDP.

#### Configuration Condition

Before configuring the basic LDP functions, do the following:

- The link layer protocol has been configured to ensure normal communication at the link layer.
- Configure address of interface at network layer so that neighbor network nodes are reachable at the network layer.
- Configure static routes or IGP protocols to ensure that each LSR can communicate at the network layer.
- Enable MPLS basic functions globally and on the interface to ensure that MPLS packets can be sent and received.

#### Enable LDP Protocol.

Table 78-3 Enabling LDP Protocol

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Enable the LDP protocol globally.	<b>mpls ldp</b>	Mandatory By default, the LDP protocol is not enabled globally.
Exit the LDP configuration mode.	<b>exit</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Enable interface LDP protocol.	<b>mpls ldp</b>	Mandatory By default, interface LDP protocol is not enabled.

## 78.2.2 Configure LDP neighbor parameters.

### Configuration Condition

Before configuring LDP neighbor parameters, do the following:

- Configure basic functions of LDP.

### Configure parameters of directly connected session.

A session established with a directly connected peer is called a directly connected LDP session.

Table 78-4 Configuring Parameters of Directly Connected Session

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the LDP configuration mode.	<b>mpls ldp</b>	Mandatory
Configure Router ID.	<b>router-id</b> <i>ip-address</i>	Optional By default, the interface address of this device is selected, and the loopback port address is preferred.

Step	Command	Description
Enter LDP IPv4 configuration mode.	<b>address-family ipv4</b>	-
Configure transport address.	<b>transport-address</b> <i>ip-address</i>	Optional By default, the Router ID is preferred as the transport address.
Exit LDP IPv4 configuration mode.	<b>exit</b>	-
Configure Keepalive message delivery interval.	<b>keepalive interval</b> <i>value</i>	Optional The default value is 60 seconds, and the range is 1~65535 seconds.
Configure Keepalive message retention timer timeout.	<b>keepalive timeout</b> <i>value</i>	Optional The default value is 180 seconds, and the range is 1~65535 seconds.
Configure link Hello sending interval.	<b>discovery hello interval</b> <i>value</i>	Optional The default value is 5 seconds, and the range is 1~65535 seconds.
Configure link Hello retention timer timeout.	<b>discovery hello holdtime</b> <i>value</i>	Optional The default value is 15 seconds, and the range is 1~65535 seconds.
Exit the LDP configuration mode.	<b>exit</b>	-
Enter interface mode.	<b>interface</b> <i>interface-name</i>	-
Configure interface link Hello sending interval.	<b>mpls ldp discovery hello interval</b> <i>value</i>	Optional The default value is 5 seconds, and the range is 1~65535 seconds.

Step	Command	Description
Configure interface link Hello retention timer timeout.	<b>mpls ldp discovery hello holdtime</b> <i>value</i>	Optional The default value is 15 seconds, and the range is 1~65535 seconds.

## Note

- To establish an LDP session between peers, you need to ensure that the LDP protocol is enabled on both peers.
- Before establishing a session with a directly connected peer, the user needs to ensure that the transport address from the local transport address to the peer is routed reachable, otherwise the session connection cannot be established.
- Modifying the Router ID or transport address can cause a successful session to be rebuilt, so it is recommended to modify the Router ID or transport address carefully.
- The sending interval and keep-alive time of link Hello can be configured globally or on the interface. When configuration is made globally and not on the interface, the transmit interval and keep-alive time of the interface link Hello use the global configuration time; when both the global and the interface have been configured, the transmit interval and keep-alive time of the interface link Hello use the interface configuration time.

### Configure remote session parameters.

The session established with the targeted peer is called a remote LDP session.

Table 78-5 Configuring Remote Session Parameters

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the LDP configuration mode.	<b>mpls ldp</b>	Mandatory
Configure Router ID.	<b>router-id</b> <i>ip-address</i>	Optional By default, the interface address of this device is selected, and the loopback port address is preferred.

Step	Command	Description
Enter LDP IPv4 configuration mode.	<b>address-family ipv4</b>	-
Create targeted peers.	<b>targeted-peer</b> <i>peer-address</i>	Mandatory No targeted peer is created by default.
Configure transport address.	<b>transport-address</b> <i>ip-address</i>	Optional By default, the Router ID is preferred as the transport address.
Exit LDP IPv4 configuration mode.	<b>exit</b>	-
Configure Keepalive message delivery interval.	<b>keepalive interval</b> <i>value</i>	Optional The default value is 60 seconds, and the range is 1~65535 seconds.
Configure Keepalive message retention timer timeout.	<b>keepalive timeout</b> <i>value</i>	Optional The default value is 180 seconds, and the range is 1~65535 seconds.
Configure the targeted Hello sending interval.	<b>discovery targeted-hello interval</b> <i>value</i>	Optional The default value is 10 seconds, and the range is 1~65535 seconds.
Configure targeted Hello retention timer timeout.	<b>discovery targeted-hello holdtime</b> <i>value</i>	Optional The default value is 90 seconds, and the range is 1~65535 seconds.

## Note

- Configure the Keepalive packet delivery interval and the timeout of the keepalive timer is applicable for both directly connected sessions and remote sessions.

- The configured Router ID and transport address are also applied to both directly connected sessions and remote sessions.
- Before establishing a session with the targeted peer, the user needs to ensure that the address route to the peer is reachable, and also needs to make sure that the targeted peer is also created on the peer end to point to the local end, otherwise the remote session cannot be established.

### 78.2.3 Configure LDP MD5 authentication.

#### Configuration Condition

Before configuring LDP neighbor parameters, do the following:

- Configure basic functions of LDP.

#### Configure LDP MD5 Authentication

To improve the security of LDP sessions, LDP sessions based on TCP connections support configuration of MD5 authentication, and only sessions with the same password on the local end and the peer end can be established.

Table 78-6 Configuring LDP MD5 Authentication

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the LDP configuration mode.	<b>mpls ldp</b>	Mandatory
Enter LDP IPv4 configuration mode.	<b>address-family ipv4</b>	-
Configure LDP MD5 authentication.	<b>peer peer-address password { 0 { password-string }   7 { password-string }   password-string }</b>	Mandatory By default, MD5 authentication password is not configured.

### 78.2.4 Configure LDP control attributes.

#### Configuration Condition

Before configuring the LDP control attributes, do the following:

- Configure basic functions of LDP.

## Configure label reception filtering.

Label reception filtering is used to filter the labels received downstream from the FEC to receive only labels from FECs that pass the access control list check. This feature can reduce the size of the MPLS forwarding table. Configure label reception filtering requires configuring a standard access control list beforehand and then using the label reception filtering command reference in the LDP.

In addition, since in most MPLS networks only the labels of FECs with 32-bit mask length are required. LDP divides FECs into two categories, i.e. 32-bit mask and non-32-bit mask, and the system only receives FEC labels with 32-bit mask length by default according to the mask length.

Table 78-7 Label Reception Filtering

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the LDP configuration mode.	<b>mpls ldp</b>	Mandatory
Enter LDP IPv4 configuration mode.	<b>address-family ipv4</b>	-
Configure label reception filtering.	<b>accept-labels for</b> <i>prefix-accesslist-name</i>	Optional By default, label reception filtering is not configured.
Configure to receive only FEC labels with a 32-bit mask length.	<b>accept-labels for</b> <b>32bit-mask-fec-only</b>	Optional By default, only FEC labels with a 32-bit mask length are received.

---

### Note

- The *prefix-accesslist-name* parameter supports only standard access control lists.
- FEC labels not filtered by access control lists will not install the corresponding FTN, but will still save and install ILM.
- By default, only labels for 32-bit mask-length FECs are received, so it is common to use the no form to configure labels for all mask-length FECs to be received.
- **accept-labels for 32bit-mask-fec-only/no accept-labels for 32bit-mask-fec-only** command and **accept-labels for** *prefix-accesslist-name* command can be configured at the same time. If the **accept-labels for 32bit-mask-fec-only** command is configured (the system default

configuration), then only FTNs of all FECs with 32-bit mask filtered by the access control list in the **accept-labels for *prefix-accesslist-name*** command will be installed, while the FTNs of all non-32-bit mask FECs will not be installed (even if the non-32-bit mask FEC passes the access control list filtering in the **accept-labels for *prefix-accesslist-name*** command); if the **no accept-labels for 32bit-mask-fec-only** command is configured, all FTNs of FECs that pass the access control list filtering in the **accept-labels for *prefix-accesslist-name*** command will be installed.

### Configure label advertisement filtering.

Label advertisement filtering is used to filter the labels of advertisement. This feature prevents LSRs from advertising a large number of labels to reduce the burden on the network. Configure label advertisement filtering requires configuring a standard access control list beforehand and then using the label advertisement filtering command reference in the LDP.

In addition, since in most MPLS networks only the labels of FECs with 32-bit mask length are required. LDP divides FECs into two categories, i.e. 32-bit mask and non-32-bit mask, and the system only advertises FEC labels with 32-bit mask length by default according to the mask length.

Table 78-8 Label Advertisement Filtering

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the LDP configuration mode.	<b>mpls ldp</b>	Mandatory
Enter LDP IPv4 configuration mode.	<b>address-family ipv4</b>	-
Configure label advertisement filtering.	<b>advertise-labels for <i>prefix-accesslist-name</i> to <i>peer-accesslist-name</i></b>	Optional By default, the label advertisement filtering function is not configured.
Configure the label for announcing partial FECs to all upstream.	<b>advertise-labels for <i>prefix-accesslist-name</i> to any</b>	Optional By default, the label advertisement filtering function is not configured.
Configure not to advertise labels to any upstream devices.	<b>advertise-labels for any to none</b>	Optional By default, no configuration is done to not advertise

Step	Command	Description
		labels to any upstream devices.
Configure labels to advertise only FECs of 32-bit mask length.	<b>advertise-labels for 32bit-mask-fec-only</b>	Optional By default, only the labels of FECs with 32-bit mask length are advertised.

## Note

- The *prefix-accesslist-name* parameter and the *peer-accesslist-name* parameter support only the standard access control lists.
- Since, by default, LDP only advertises the labels of 32-bit mask-length FECs upstream, it is generally configured to advertise the labels of all mask-length FECs upstream using its no form.
- The **advertise-labels for any to none** command and the **advertise-labels for *prefix-accesslist-name* to any** command can be viewed as special forms of the **advertise-labels *prefix-accesslist-name* to *peer-accesslist-name*** command, **any** means to permit any, and **none** means to deny any. All three sets of commands can be used to enable control label advertisement via access control lists, and can be configured at the same time as the **adjustise-labels-for-32bit-mask-fec-only** command.
- If the **adverse-labels for 32bit-mask-fec-only** command is configured (system default), all non-32bit-mask FECs are denied of label advertisement, while 32bit-mask FECs will undergo lable advertisement according to the results of access control list checks. If the **no advertise-labels for 32bit-mask-fec-only** command is configured, all mask-length FECs will will undergo lable advertisement according to the result of the access control list check.

### Configuration label re-advertisement.

After label re-advertisement is configured, LDP periodically re-advertises all label images to upstream neighbors.

Table 9-10 Label Re-Advertisement

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the LDP configuration mode.	<b>mpls ldp</b>	Mandatory

Step	Command	Description
Configuration label re-advertisement.	<b>du-readvertise</b>	Mandatory By default, label mapping is not re-advertised.
Configure the re-advertisement interval.	<b>du-readvertise timer value</b>	Optional The default value is 30 seconds, the range is 1~65535 seconds.

### Configure label assignment control method.

The label assignment control method of LDP refers to the processing method used by the LSR to assign labels during the establishment of the LSP.

Independent label assignment control means that the local LSR can autonomously assign a label binding to a certain FEC and advertise it to the upstream LSR without waiting for the downstream label.

The ordered allocation label control method means that for the label mapping of a FEC on an LSR, the LSR can send the label mapping of this FEC upstream only if the LSR already has the label mapping message for the next hop of this FEC or if the LSR is the outgoing node of this FEC.

Table 11-12 Configuring the Label Assignment Control Method

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the LDP configuration mode.	<b>mpls ldp</b>	-
Configure the ordered assignment control method for labels.	<b>label-distribution ordered</b>	Optional Default is independent label assignment control method.
Configure the independent assignment control method for labels.	<b>label-distribution independent</b>	Optional Default is independent label assignment control method.

### Configure PHP features.

When the device acts as an Egress node, the implicit null label is distributed to the penultimate hop device by default. After the **explicit-null** command is configured the Egress node sends the display null label to the penultimate hop device. If the Egress node distributes an implicit empty label, the label will pop up on the penultimate hop, and if the Egress node distributes a display empty label, the label will not pop up on the penultimate hop device.

Table 78-13 Configuring PHP Features

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the LDP configuration mode.	<b>mpls ldp</b>	Mandatory
Configure Egress nodes to display empty labels to upstream advertisement.	<b>explicit-null</b>	Optional By default, the Egress node advertises an implicit empty label to the penultimate hop.

---

### Note

- To configure or delete the **explicit-null** command, you need to reset the session with the **clear mpls ldp session** command for the command to take effect.
- 

### Configure loopback detection.

There are two ways to detect LSP loops, a maximum hop count way and a path vector way.

The maximum hop count approach is to include the hop value in the message passing the label, and add one to that value for each LSR passed. When this value reaches the maximum value detected, a loop is considered to occur and the LSP establishment process is terminated.

The path vector approach, on the other hand, records LSR ID information in the message passing the label, and each time a hop is passed, the corresponding device checks whether its own LSR ID has been recorded.

If the record does not have its own LSR ID, it adds its own LSR ID to the record; if the record already has its own LSR ID, it assumes that a loop has occurred and terminates the LSP establishment process.

Table 78-14 Configuring Loopback Detection

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the LDP configuration mode.	<b>mpls ldp</b>	Mandatory
Configure Loop Detection	<b>loop-detection</b>	Mandatory By default, no loop detection is configured.
Configure the maximum number of hops for loop detection.	<b>maxhops value</b>	Optional In the configuration of loopback detection after the default detection hop limit value is 255, configurable range is 1 ~ 255.

---

 **Note**

- The loop detection configuration on the LDP peer must be consistent, otherwise the LDP session cannot be established.
  - After configuring loop detection, LDP immediately detects LSP loops using both maximum hop count and path vector, where the maximum hop count is the default value of 255 hops.
- 

**Configure session reconnection.**

When a TCP connection with a peer is established unsuccessfully, LDP tries to re-establish it, a process called session reconnection.

Table 78-15 Session Reconnection Capability

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the LDP configuration mode.	<b>mpls ldp</b>	Mandatory
Configure not to allow increased reconnection delay time.	<b>reconnection-delay-disable</b>	Optional By default, the reconnection delay time is allowed to increase.
Configure the initial value of the reconnection interval.	<b>reconnect-interval</b> <i>value</i>	Optional The default value is 15 seconds, the value range is 1~15 seconds.

---

### Note

- The initial value of the delay time of LDP reconnect peer is 15 seconds, if allowed to increase the reconnection delay time, then the delay time will be doubled one by one after the failure of initiating TCP connection to the peer, which is 15 seconds, 30 seconds, 60 seconds, 120 seconds in order, and the maximum will not exceed 120 seconds; if the initial value of the delay time of LDP reconnect peer is 1 second, the reconnection delay time will be 1 second, 2 seconds, 4 seconds ..... in that order, and the maximum will not exceed 120 seconds. If the reconnection delay time is not enabled to increase, the reconnection interval will always be the initial value of the configured reconnection interval.
- 

## 78.2.5 Configure LDP GR.

### Configuration Condition

Before configuring LDP GR capabilities, do the following:

- Configure basic functions of LDP.
- Before configuring LDP GR capabilities, first complete the following tasks.

### Configure LDP GR

LDP GR takes advantage of the separation of MPLS forwarding plane and control plane to keep the MPLS label forwarding table entry in case of abnormality in the control plane, and LSR still forwards packets according to the table entry, thus ensuring that data transmission will not be interrupted.

During GR, the devices in the MPLS network are divided into two roles.

- GR restarter: GR restart router, refers to a device with dual master control that triggers a control level restart protocol due to user manual or failure.
- GR helper: A neighbor of the GR restarter that maintains a neighbor relationship with the restarted GR restarter and has negotiated GR capabilities with the GR restarter to assist it in restoring the pre-restart forwarding state after the GR restarter restarts.

The work process of LDP GR is as follows.

- When the session between neighbors is established at first, the time value of each GR timer is negotiated between the LSRs configured with GR capability.
- After a restart occurs in the GR restarter, the GR helper detects a session down with the GR restarter, marks all label mappings learned through this session as stale, and retains these label mappings for the GR neighbor keep-alive timer timeout.
- If the neighbor keep-alive timer times out, GR Helper removes these label mappings marked as stale. If the LDP session is successfully established within the GR neighbor preservation timer timeout, the GR restarter and GR helper update the label forwarding table and clear the stale label of the forwarding table entry by interacting the label mapping with the newly established LDP session during the LDP recovery time. After the LDP recovery timer times out, the GR helper removes the label mappings that are still marked as stale.
- The MPLS forwarding state hold timer timeout indicates the end of the GR process.

Table 78-16 Configuring LDP GR

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the LDP configuration mode.	<b>mpls ldp</b>	Mandatory
Enabling GR capability	<b>graceful-restart</b>	Mandatory By default, no GR capability is enabled.
Configure the GR forwarding state hold timer timeout.	<b>graceful-restart timer forwarding-holding value</b>	Optional

Step	Command	Description
		The default value is 300 seconds, the value range is 30~300 seconds.
Configure the GR recovery timer timeout.	<b>graceful-restart timer max-recovery value</b>	Optional The default value is 120 seconds, the value range is 15~600 seconds.
Configure the GR Neighbor Keep Alive timer timeout.	<b>graceful-restart timer neighbor-liveness value</b>	Optional The default value is 120 seconds, the value range is 5~300 seconds.

---

## Note

- GR needs to be configured on both peers of the session before the LDP session is established in order to negotiate a successful GR capability. LDP sessions established before GR capability is enabled do not have GR capability.
- 

### 78.2.6 Configure LDP to coordinate with BFD.

#### Configuration Condition

Before configuring LDP with BFD linkage, do the following:

- Configure basic functions of LDP.
- Enable the LDP protocol on the interface that needs to be configured for LDP and BFD linkage.

#### Configure LDP to coordinate with BFD.

When there is a line failure between two neighboring devices, it takes longer for LDP to detect the neighboring line failure, and after the line failure is detected, the LDP session goes down and MPLS forwarding is interrupted. LDP and BFD linkage can quickly detect line failures of LDP neighbors and improve the performance of MPLS networks.

Table 78-17 Configuring LDP and BFD Linkage

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the LDP configuration mode.	<b>mpls ldp</b>	Mandatory
Configure globally to enable coordination between LDP and BFD.	<b>bfd all-interfaces</b>	Optional By default, the LDP and BFD linkage is not enabled globally.
Exit the LDP configuration mode.	<b>exit</b>	-
Enter the interface configuration mode	<b>interface <i>interface-name</i></b>	Mandatory
Configure the interface to enable coordination between LDP and BFD.	<b>mpls ldp bfd</b>	Optional By default, LDP and BFD linkage are not enabled on the interface.
Configure the interface to disable coordination between LDP and BFD.	<b>mpls ldp bfd disable</b>	Optional By default, the interface is allowed to enable LDP with BFD linkage.

---

## Note

- For the configuration of BFD, refer to contents on BFD in the Reliability section in the User Manual.
  - The current LDP only supports single-hop detection results linked with BFD, and does not support multi-hop detection results.
  - The **mpls ldp bfd disable** command on the interface is mutually exclusive with the **mpls ldp bfd** command and has a higher priority than the **bfd all-interfaces** command in MPLS LDP mode. The impact of various combinations of configurations between them on the results of enabling the interface LDP and BFD linkage is shown in the following table.
-

bfd all-interfaces	mpls ldp bfd	mpls ldp bfd disable	Enabling LDP and BFD linkage on an interface.
18.5.2 Configuration	Not configured or no drop	Not configured or no drop	Enabled
18.5.2 Configuration	Not configured or no drop	18.5.2 Configuration	Not enabled
18.5.2 Configuration	18.5.2 Configuration	Not configured or no drop	Enabled
Not configured or no drop	Not configured or no drop	Not configured or no drop	Not enabled
Not configured or no drop	Not configured or no drop	18.5.2 Configuration	Not enabled
Not configured or no drop	18.5.2 Configuration	Not configured or no drop	Enabled

## 78.2.7 LDP Monitoring and Maintaining

Table 78-20 List of LDP Monitoring and Maintaining Commands

Command	Description
<b>clear mpls ldp adjacency</b> { <i>ip-address</i>   all }	Reset all LDP adjacencies or specify an adjacency.
<b>clear mpls ldp error-statistics</b>	Clear the error statistics of LDP.
<b>clear mpls ldp session</b> { <i>peer-address</i>   all }	Reset all LDP sessions or sessions of the specified peer.
<b>clear mpls ldp statistics</b>	Clear statistics on LDP messages sent and received.
<b>clear mpls ldp statistics advertise-labels</b> [ for <i>prefix-accesslist-name</i> [ to <i>peer-accesslist-name</i> ] ]	Clear statistics for LDP label advertisement filtering.

Command	Description
<b>show mpls ldp adjacency</b>	Display information about all LDP adjacencies.
<b>show mpls ldp advertise-labels</b>	Display statistics for LDP label advertisement filtering.
<b>show mpls ldp downstream</b> [ <i>prefix-address prefixlen</i> ]	Display all downstream information of LDP or downstream information of specified FEC.
<b>show mpls ldp error-statistics</b>	Display error statistics for LDP.
<b>show mpls ldp fec</b> [ <i>prefix-address prefixlen</i> ]	Display information about all FECs of LDP or FECs with specified prefixes.
<b>show mpls ldp fec number</b>	Display the number of FEC of LDP.
<b>show mpls ldp interface</b> [ <i>interface-name</i> ]	Show details of all LDP interfaces or specified LDP interfaces.
<b>show mpls ldp lsp</b> [ <b>advertise-list</b>   <i>prefix-address prefixlen</i> [ <b>advertise-list</b> ] ]	Display LSP details for all LSPs of LDP or FECs of the specified prefix.
<b>show mpls ldp parameter</b> [ <b>detail</b> ]	Display the parameters of LDP.
<b>show mpls ldp session</b> [ <b>statistics</b>   <i>peer-address</i> [ <b>detail</b> ] ]	Displays LDP sessions and related statistics or details of the specified session.
<b>show mpls ldp statistics message</b>	Display statistics of LDP packets sent and received.
<b>show mpls ldp statistics advertise-labels</b>	Display statistics for LDP label advertisement.
<b>show mpls ldp targeted-peers</b>	Display information about all target peers of LDP.
<b>show mpls ldp upstream</b> [ <i>prefix-address prefixlen</i> ]	Display upstream information for all LDP upstream or specified FECs.

## 78.3 MPLS LDP Typical Configuration Example

### 78.3.1 Configure basic functions of LDP.

#### Network Requirements

- The entire network uses OSPF interactive routing.
- The device enables MPLS IP and MPLS LDP, and LDP sessions are established between Device1 and Device2, Device2 and Device3.

#### Network Topology

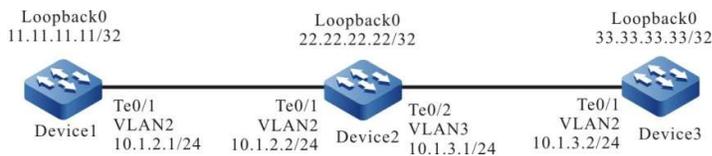


Figure 1-2 Network Topology for Configuring Basic Functions of LDP.

#### Configuration Steps

- Step 1: Configure the VLAN and add the port to the corresponding VLAN in access mode. (Omitted)
- Step 2: Configure IP addresses for the ports. (Omitted)
- Step 3: Configure OSPF.

#### #Configure OSPF on Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#network 10.1.2.0 0.0.0.255 area 0
Device1(config-ospf)#network 11.11.11.11 0.0.0.0 area 0
Device1(config-ospf)#exit
```

#### #Configure OSPF on Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 10.1.2.0 0.0.0.255 area 0
Device2(config-ospf)#network 10.1.3.0 0.0.0.255 area 0
Device2(config-ospf)#network 22.22.22.22 0.0.0.0 area 0
Device2(config-ospf)#exit
```

#### #OSPF deployed on Device3.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#network 10.1.3.0 0.0.0.255 area 0
Device3(config-ospf)#network 33.33.33.33 0.0.0.0 area 0
Device3(config-ospf)#exit
```

#View the routing table on each device.

Here takes Device1 for example:

```
Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
C 10.1.2.0/24 is directly connected, 06:19:07, vlan2
L 10.1.2.1/32 is directly connected, 06:19:07, vlan2
O 10.1.3.0/24 [110/2] via 10.1.2.2, 06:05:08, vlan2
LC 11.11.11.11/32 is directly connected, 06:18:54, loopback0
O 22.22.22.22/32 [110/2] via 10.1.2.2, 06:12:40, vlan2
O 33.33.33.33/32 [110/3] via 10.1.2.2, 06:02:59, vlan2
C 127.0.0.0/8 is directly connected, 102:05:13, lo0
L 127.0.0.1/32 is directly connected, 102:05:13, lo0
```

It is indicated that the routing table of Device1 has routes to the loopback0 interface of Device2 and Device3.

---

## Note

- Refer to Device1 for the checking method for Device2 and Device3.
- 

Step 4: Enable MPLS IP and MPLS LDP.

# Enable MPLS IP and MPLS LDP globally on Device1, and also enable MPLS IP and MPLS LDP on the interface.

```
Device1(config)#mpls ip
Device1(config)#mpls ldp
Device1(config-ldp)#router-id 11.11.11.11
```

```
Device1(config-ldp)#address-family ipv4
Device1(config-ldp-af4)#transport-address 11.11.11.11
Device1(config-ldp-af4)#exit
Device1(config-ldp)#exit
Device1(config)#interface vlan2
Device1(config-if-vlan2)#mpls ip
Device1(config-if-vlan2)#mpls ldp
Device1(config-if-vlan2)#exit
```

# Enable MPLS IP and MPLS LDP globally on Device2, and also enable MPLS IP and MPLS LDP on the interface.

```
Device2(config)#mpls ip
Device2(config)#mpls ldp
Device2(config-ldp)#router-id 22.22.22.22
Device2(config-ldp)#address-family ipv4
Device2(config-ldp-af4)#transport-address 22.22.22.22
Device2(config-ldp-af4)#exit
Device2(config-ldp)#exit
Device2(config)#interface vlan2
Device2(config-if-vlan2)#mpls ip
Device2(config-if-vlan2)#mpls ldp
Device2(config-if-vlan2)#exit
Device2(config)#interface vlan3
Device2(config-if-vlan3)#mpls ip
Device2(config-if-vlan3)#mpls ldp
Device2(config-if-vlan3)#exit
```

# Enable MPLS IP and MPLS LDP globally on Device3, and also enable MPLS IP and MPLS LDP on the interface.

```
Device3(config)#mpls ip
Device3(config)#mpls ldp
Device3(config-ldp)#router-id 33.33.33.33
Device3(config-ldp)#address-family ipv4
Device3(config-ldp-af4)#transport-address 33.33.33.33
Device3(config-ldp-af4)#exit
Device3(config-ldp)#exit
Device3(config)#interface vlan2
Device3(config-if-vlan2)#mpls ip
Device3(config-if-vlan2)#mpls ldp
Device3(config-if-vlan2)#exit
```

---

## Note

- router-id and transport-address can be manually configured or automatically generated, and are generally configured to be the same. If router-id and transport-address are not manually configured, the device will automatically select them. Among the interfaces in the up state, the largest IP address in the Loopback interface is selected first; if the device is not configured with a Loopback interface address, the largest IP address in the normal interface is selected.
- 

Step 5: Check the result.

# View LDP session information on individual devices.

Here takes Device1 for example:

```
Device1#show mpls ldp session
Peer IP Address  Peer Type  My Role  State      DS Cap  DeadTime
22.22.22.22     Multicast  Passive  OPERATIONAL Disabled 00:02:01

Statistics for ldp sessions:
  Multicast sessions: 1
  Targeted sessions: 0
```

The content of the State column is shown as OPERATIONAL, which shows that Device1 and Device2 successfully established an LDP session.

# View the routing label information on the device.

Here takes Device1 for example:

```
Device1#show ip route 22.22.22.22 detail
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

O 22.22.22.22/32 [110/2] via 10.1.2.2, label 3, 14:29:21, vlan2
   10.1.2.2 [0], vlan2

Device1#show ip route 33.33.33.33 detail
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
O 33.33.33.33/32 [110/3] via 10.1.2.2, label 17, 14:29:21, vlan2
    10.1.2.2 [0], vlan2
```

It is indicated the routing label information in Device1 to the loopback0 interface address of Device2 and Device3.

# View LSP information on individual devices.

Here takes Device1 for example:

```
Device1#show mpls ldp lsp

FEC IPV4:10.1.2.0/24 -> 0.0.0.0, vlan2
FEC IPV4:10.1.3.0/24 -> 10.1.2.2, vlan2

FEC IPV4:11.11.11.11/32 -> 0.0.0.0, loopback0
  Downstream state: Established Label: none      RequestID: 0 Peer: EGRESS Attr: None
  Upstream state: Established Label: impl-null(3) RequestID: 0 Peer: 22.22.22.22 Attr: None

FEC IPV4:22.22.22.22/32 -> 10.1.2.2, vlan2
  Downstream state: Established Label: impl-null(3) RequestID: 0 Peer: 22.22.22.22 Attr: None

FEC IPV4:33.33.33.33/32 -> 10.1.2.2, vlan2
  Downstream state: Established Label: 17      RequestID: 0 Peer: 22.22.22.22 Attr: None
```

It is indicated that the information of the loopback0 interface address of Device2 and Device3 corresponding to the LSP of FEC exists on Device1.

---

## Note

- Refer to Device1 for the checking method for Device2 and Device3.
- 

## 78.3.2 Configuring LDP remote sessions.

### Network Requirements

- The entire network uses OSPF interactive routing.

- Device1 and Device3 enable MPLS IP and MPLS LDP, and LDP remote sessions are established between Device1 and Device3.

### Network Topology

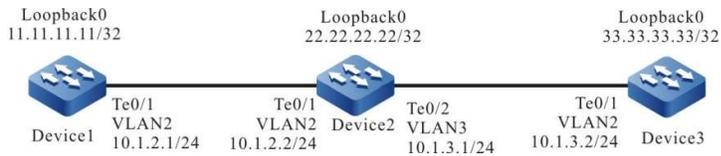


Figure 3-4 Network Topology for Configuring LDP Remote Session

### Configuration Steps

- Step 1: Configure the VLAN and add the port to the corresponding VLAN in access mode. (Omitted)
- Step 2: Configure IP addresses for the ports. (Omitted)
- Step 3: Configure OSPF.

#Configure OSPF on Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#network 10.1.2.0 0.0.0.255 area 0
Device1(config-ospf)#network 11.11.11.11 0.0.0.0 area 0
Device1(config-ospf)#exit
```

#Configure OSPF on Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 10.1.2.0 0.0.0.255 area 0
Device2(config-ospf)#network 10.1.3.0 0.0.0.255 area 0
Device2(config-ospf)#network 22.22.22.22 0.0.0.0 area 0
Device2(config-ospf)#exit
```

#OSPF deployed on Device3.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#network 10.1.3.0 0.0.0.255 area 0
Device3(config-ospf)#network 33.33.33.33 0.0.0.0 area 0
Device3(config-ospf)#exit
```

#View the routing table on each device.

Here takes Device1 for example:

```
Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
C 10.1.2.0/24 is directly connected, 06:19:07, vlan2
L 10.1.2.1/32 is directly connected, 06:19:07, vlan2
O 10.1.3.0/24 [110/2] via 10.1.2.2, 06:05:08, vlan2
LC 11.11.11.11/32 is directly connected, 06:18:54, loopback0
O 22.22.22.22/32 [110/2] via 10.1.2.2, 06:12:40, vlan2
O 33.33.33.33/32 [110/3] via 10.1.2.2, 06:02:59, vlan2
C 127.0.0.0/8 is directly connected, 102:05:13, lo0
L 127.0.0.1/32 is directly connected, 102:05:13, lo0
```

It is indicated that the routing table of Device1 has routes to the loopback0 interface of Device2 and Device3.

---

## Note

- Refer to Device1 for the checking method for Device2 and Device3.
- 

Step 4: Enable MPLS IP and MPLS LDP, and configure remote LDP sessions.

#Enable MPLS IP and MPLS LDP globally on Device1, and also enable MPLS IP and MPLS LDP on the interface, and configure the remote LDP peer.

```
Device1(config)#mpls ip
Device1(config)#mpls ldp
Device1(config-ldp)#router-id 11.11.11.11
Device1(config-ldp)#address-family ipv4
Device1(config-ldp-af4)#transport-address 11.11.11.11
Device1(config-ldp-af4)#targeted-peer 33.33.33.33
Device1(config-ldp-af4)#exit
Device1(config-ldp)#exit
Device1(config)#interface vlan2
Device1(config-if-vlan2)#mpls ip
```

```
Device1(config-if-vlan2)#mpls ldp
Device1(config-if-vlan2)#exit
```

#Enable MPLS IP and MPLS LDP globally on Device3, and also enable MPLS IP and MPLS LDP on the interface, and configure the remote LDP peer.

```
Device3(config)#mpls ip
Device3(config)#mpls ldp
Device3(config-ldp)#router-id 33.33.33.33
Device3(config-ldp)#address-family ipv4
Device3(config-ldp-af4)#transport-address 33.33.33.33
Device3(config-ldp-af4)#targeted-peer 11.11.11.11
Device3(config-ldp-af4)#exit
Device3(config-ldp)#exit
Device3(config)#interface vlan2
Device3(config-if-vlan2)#mpls ip
Device3(config-if-vlan2)#mpls ldp
Device3(config-if-vlan2)#exit
```

Step 5: Check the result.

# View remote LDP session information on Device1 and Device3.

Here takes Device1 for example:

```
Device1#show mpls ldp session
Peer IP Address  Peer Type  My Role  State    DS Cap  DeadTime
33.33.33.33     Targeted  Passive  OPERATIONAL  Disabled 00:02:57
Statistics for ldp sessions:
  Multicast sessions: 0
  Targeted sessions: 1
```

Device1 and Device3 successfully established a remote LDP session as shown by the content of the State column as OPERATIONAL and the content of the Peer Type column as Targeted.

# View LDP adjacencies on Device1, Device3.

Here takes Device1 for example:

```
Device1#show mpls ldp adjacency
IP Address  Interface Name  DS Cap  Deadtme  LDP-Identifier
33.33.33.33  /              Disable  00:01:20  33.33.33.33:0
```

In the LDP neighbor table of Device1, It is indicated the Targeted neighbor 33.33.33.33 with the interface name "/".

# View remote peers on Device1, Device3.

Here takes Device1 for example:

```
Device1#show mpls ldp targeted-peers
IP Address      State
33.33.33.33    Active
```

It is indicated that there is information about Device3 in the Device1 remote peer table.

---

## Note

- For Device3 check method, refer to Device1.
- 

### 78.3.3 Configure to enable coordination between MPLS LDP and BFD.

#### Network Requirements

- The whole network uses OSPF interactive routing, the device enables MPLS IP and MPLS LDP, and Device1 and Device3 is configured to enable coordination between MPLS LDP and BFD.
- When the line between Device1 and Device3 fails, the MPLS service data between Device1 and Device3 can be quickly switched.

#### Network Topology

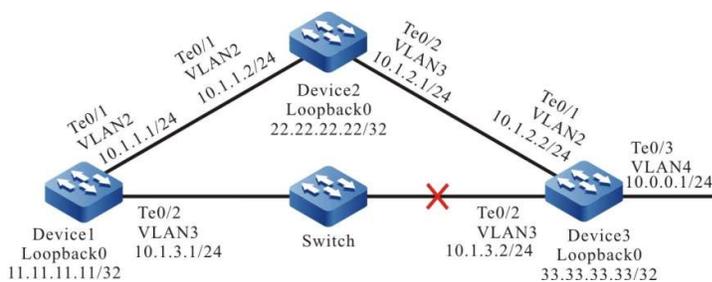


Figure 78-5 Configuring to Enable Coordination between MPLS LDP and BFD

#### Configuration Steps

- Step 1: Configure the VLAN and add the port to the corresponding VLAN in access mode. (Omitted)
- Step 2: Configure IP addresses for the ports. (Omitted)

### Step 3: Configure OSPF.

#### #Configure OSPF on Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#network 10.1.1.0 0.0.0.255 area 0
Device1(config-ospf)#network 10.1.3.0 0.0.0.255 area 0
Device1(config-ospf)#network 11.11.11.11 0.0.0.0 area 0
Device1(config-ospf)#exit
```

#### #Configure OSPF on Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 10.1.1.0 0.0.0.255 area 0
Device2(config-ospf)#network 10.1.2.0 0.0.0.255 area 0
Device2(config-ospf)#network 22.22.22.22 0.0.0.0 area 0
Device2(config-ospf)#exit
```

#### #OSPF deployed on Device3.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#network 10.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 10.1.2.0 0.0.0.255 area 0
Device3(config-ospf)#network 10.1.3.0 0.0.0.255 area 0
Device3(config-ospf)#network 33.33.33.33 0.0.0.0 area 0
Device3(config-ospf)#exit
```

#### #View the routing table on each device.

Here takes Device1 for example:

```
Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

O 10.0.0.0/24 [110/2] via 10.1.3.2, 00:12:57, vlan3
C 10.1.1.0/24 is directly connected, 02:22:00, vlan2
L 10.1.1.1/32 is directly connected, 02:22:00, vlan2
O 10.1.2.0/24 [110/2] via 10.1.1.2, 02:00:31, vlan2
  [110/2] via 10.1.3.2, 00:12:57, vlan2
```

```
C 10.1.3.0/24 is directly connected, 02:21:47, vlan3
L 10.1.3.1/32 is directly connected, 02:21:47, vlan3
LC 11.11.11.11/32 is directly connected, 02:16:48, loopback0
O 22.22.22.22/32 [110/2] via 10.1.1.2, 02:00:21, vlan2
O 33.33.33.33/32 [110/2] via 10.1.3.2, 00:12:57, vlan3
C 127.0.0.0/8 is directly connected, 483:17:24, lo0
L 127.0.0.1/32 is directly connected, 483:17:24, lo0
```

It is indicated that Device1's routing table has a route to Device3's directly connected segment 10.0.0.0/24, and the line between Device1 and Device3 is preferred for communication.

---

## Note

- Refer to Device1 for the inspection method of Device2 and Device3.
- 

Step 4: Enable MPLS IP and MPLS LDP.

# Enable MPLS IP and MPLS LDP globally on Device1, enable MPLS IP and MPLS LDP on the interface at the same time, and remove the 32-bit mask FEC assignment and receive labels only under the MPLS LDP process.

```
Device1(config)#mpls ip
Device1(config)#mpls ldp
Device1(config-ldp)#router-id 11.11.11.11
Device1(config-ldp)#address-family ipv4
Device1(config-ldp-af4)#transport-address 11.11.11.11
Device1(config-ldp-af4)#no advertise-labels for 32bit-mask-fec-only
Device1(config-ldp-af4)#no accept-labels for 32bit-mask-fec-only
Device1(config-ldp-af4)#exit
Device1(config-ldp)#exit
Device1(config)#interface vlan2
Device1(config-if-vlan2)#mpls ip
Device1(config-if-vlan2)#mpls ldp
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan3
Device1(config-if-vlan3)#mpls ip
Device1(config-if-vlan3)#mpls ldp
Device1(config-if-vlan3)#exit
```

# Enable MPLS IP and MPLS LDP globally on Device2, enable MPLS IP and MPLS LDP on the interface at the same time, and remove the 32-bit mask FEC assignment and receive labels only under the MPLS LDP process.

```
Device2(config)#mpls ip
Device2(config)#mpls ldp
Device2(config-ldp)#router-id 22.22.22.22
Device2(config-ldp)#address-family ipv4
Device2(config-ldp-af4)#transport-address 22.22.22.22
Device2(config-ldp-af4)#no advertise-labels for 32bit-mask-fec-only
Device2(config-ldp-af4)#no accept-labels for 32bit-mask-fec-only
Device2(config-ldp-af4)#exit
Device2(config-ldp)#exit
Device2(config)#interface vlan2
Device2(config-if-vlan2)#mpls ip
Device2(config-if-vlan2)#mpls ldp
Device2(config-if-vlan2)#exit
Device2(config)#interface vlan3
Device2(config-if-vlan3)#mpls ip
Device2(config-if-vlan3)#mpls ldp
Device2(config-if-vlan3)#exit
```

# Enable MPLS IP and MPLS LDP globally on Device3, enable both MPLS IP and MPLS LDP on the interface, and remove the 32-bit mask FEC assignment and receive labels only under the MPLS LDP process.

```
Device3(config)#mpls ip
Device3(config)#mpls ldp
Device3(config-ldp)#router-id 33.33.33.33
Device3(config-ldp)#address-family ipv4
Device3(config-ldp-af4)#transport-address 33.33.33.33
Device3(config-ldp-af4)#no advertise-labels for 32bit-mask-fec-only
Device3(config-ldp-af4)#no accept-labels for 32bit-mask-fec-only
Device3(config-ldp-af4)#exit
Device3(config-ldp)#exit
Device3(config)#interface vlan2
Device3(config-if-vlan2)#mpls ip
Device3(config-if-vlan2)#mpls ldp
Device3(config-if-vlan2)#exit
Device3(config)#interface vlan3
Device3(config-if-vlan3)#mpls ip
Device3(config-if-vlan3)#mpls ldp
Device3(config-if-vlan3)#exit
Device3(config)#interface vlan4
```

```

Device3(config-if-vlan4)#mpls ip
Device3(config-if-vlan4)#mpls ldp
Device3(config-if-vlan4)#exit

```

# View LDP session information on individual devices.

Here takes Device1 for example:

```

Device1#show mpls ldp session
Peer IP Address  Peer Type  My Role  State      DS Cap  DeadTime
22.22.22.22     Multicast  Passive  OPERATIONAL Disabled 00:02:54
33.33.33.33     Multicast  Passive  OPERATIONAL Disabled 00:02:41

Statistics for ldp sessions:
  Multicast sessions: 2
  Targeted sessions: 0

```

The content of the State column is shown as OPERATIONAL, which shows that Device1 has successfully established LDP sessions with Device2 and Device3.

#View the MPLS forwarding table on each device.

Here takes Device1 for example:

```

Device1#show ip route 10.0.0.1 detail
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

O 10.0.0.0/24 [110/2] via 10.1.3.2, label 3, 14:29:21, vlan3
    10.1.3.2 [0], vlan3

Device1#show mpls forwarding-table ilm 10.0.0.1 24
Pro: L - LDP, B - MP-BGP, R - RSVP, M - Mapped-Route, ML - mLDP (ML FEC: Root
address/OT/OV), RM - RSVP P2MP (RM FEC: P2MP ID/TID)

Pro Ident      FEC          Inlabel Outlabel Outgoing      Next hop
L global      10.0.0.0/24  20  3  vlan3         10.1.3.2

```

It is indicated that there is routing label information on Device1 to Device3 directly connected segment 10.0.0.0/24, and the line between Device1 and Device3 is preferred for communication.

---

## Note

- By default, the device is enabled under the MPLS LDP process to assign and receive labels with 32-bit mask FEC only.
  - Refer to Device1 for the inspection method of Device2 and Device3.
- 

Step 5: Configure to enable coordination between OSPF, LDP and BFD.

#Configure to enable coordination between OSPF, LDP and BFD on Device1.

```
Device1(config)#interface vlan3
Device1(config-if-vlan3)#ip ospf bfd
Device1(config-if-vlan3)#mpls ldp bfd
Device1(config-if-vlan3)#exit
```

#Configure to enable coordination between OSPF, LDP and BFD on Device3.

```
Device3(config)#interface vlan3
Device3(config-if-vlan3)#ip ospf bfd
Device3(config-if-vlan3)#mpls ldp bfd
Device3(config-if-vlan3)#exit
```

Step 6: Check the result.

#View the BFD session information of Device1 and Device3.

Here takes Device1 for example:

```
Device1#show bfd session detail
Total session number: 1
OurAddr      NeighAddr    LD/RD      State  Holddown  Interface
10.1.3.1     10.1.3.2     6/4        UP     5000     vlan3
Type:ipv4 direct
Local State:UP Remote State:UP Up for: 0h:36m:4s Number of times UP:1
Send Interval:1000ms Detection time:5000ms(1000ms*5)
Local Diag:0 Demand mode:0 Poll bit:0
MinTxInt:1000 MinRxInt:1000 Multiplier:5
Remote MinTxInt:1000 Remote MinRxInt:1000 Remote Multiplier:5
Registered protocols:LDP OSPF
```

It is indicated that OSPF, LDP and BFD are successfully linked and the session is established normally.

# When a line failure occurs between Device1 and Device3, BFD quickly detects and notifies OSPF and LDP for fast convergence to see the route label information of each device.

Here takes Device1 for example:

```
Device1#show ip route 10.0.0.1 detail
```

```
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
```

```
U - Per-user Static route
```

```
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
O 10.0.0.0/24 [110/3] via 10.1.1.2, label 21, 00:12:48, vlan2  
    10.1.1.2 [0], vlan2
```

In the routing table, It is indicated that to route 10.0.0.0/24 select the line between Device1 and Device2 for communication.

---

## Note

- Refer to Device1 for the inspection method of Device3.
-

# 79 MPLS L3VPN

## 79.1 Overview

MPLS L3VPN is a network technology that allows service providers to use their IP backbones to provide Layer 3 VPN services to their subscribers. In an MPLS L3VPN network, BGP is used to publish VPN routing information in the service provider backbone and MPLS is used to forward VPN services from one VPN site to another.

VPN Routing/Forwarding Instance (VRF) is a fundamental concept in MPLS L3VPN network technology. Each VRF can be seen as a virtual router with a separate routing table, while the VRF also has a separate address space, a set of interfaces belonging to the VRF, and a set of routing protocols used only for that VRF. VRF technology can be used to isolate different VPN users and solve the problem of overlapping network addresses.

The following diagram shows the MPLS L3VPN network structure.

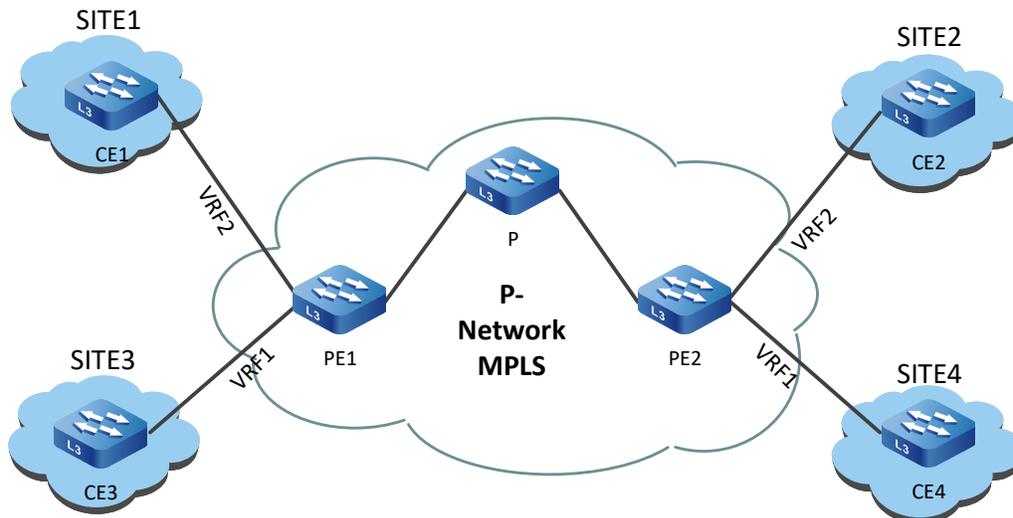


Figure 79-1 Network Topology for MPLS L3VPN

In the above figure, each PE contains two VRFs connecting 2 sites, and the 2 interfaces connecting the sites belong to each of the 2 VRFs. Site 1 and Site 2 belong to one VPN, and Site 3 and Site 4 belong to another VPN.

## 79.2 MPLS L3VPN Function Configuration

Table 79-1 MPLS L3VPN Function Configuration List

Configuration Task	
Configure basic functions of VPN.	Configure VPN instances.
	Configure PE-PE inter-route switching.
	Configure PE-CE inter-route switching.
Configure M-VRF.	Configure M-VRF.
Configure VPN route label assignment.	Configure VPN route label assignment.
Configure VPN to cross domain.	Configure Option-A to cross domain.
	Configure Option-B to cross domain.
Configure VPN users to access the Internet.	Configure CE access to the Internet.
	Configure PE access to the Internet.
Configure AS override.	Configure AS override.
Configure OSPF Pseudo-Connections	Configure OSPF Pseudo-Connections

### 79.2.1 Configure basic functions of VPN.

#### Configuration Condition

Before configuring basic VPN functions, do the following:

- Configure the MPLS backbone IGP to achieve IP reachability between PE and PE devices.
- Configure the MPLS basic capability and LDP of the MPLS backbone, and establish LSPs between PEs and PE devices.

#### Configure VPN instances.

VRF can isolate the routes between different VPNs and between VPN and public network. When configuring L3VPN, you need to configure VPN instance on PE device and associate Site (site) in VPN instance.

## 1. Configure VRF

VRFs are used to isolate different VPN users, and address overlap is allowed in different VRFs. When VRF routes are passed through the service provider network, the problem of address overlap must be solved, which requires a locally unique RD for each VRF. When the PE sends the VRF route to the remote PE, it will add RD in front of each IPv4 prefix to form a unique VPNv4 address.

Table 2-3 Configuring the VRF

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Create VRF and enter VRF configuration mode	<b>ip vrf vrf-name</b>	Mandatory By default, no VRF is configured.
Configure RD for VRF.	<b>rd route-distinguisher</b>	Mandatory By default, RD for VRF is not configured.

---

### Note

- The RD must be configured at the same time after the VRF is configured for the VRF to be used.
  - After RD for VRF is configured, it cannot be deleted or modified directly, and when it must be deleted or modified, you need to delete the VRF through the **no ip vrf** command and then configure the RD, and the RD cannot be the same as the RD of other VRFs in this device.
- 

## 2. Configure to Associate VRF with Interface

The PE device is connected to the CE through a locally configured VRF, and the interface connected to the CE needs to be associated to the corresponding VRF.

Table 79-4 Configuring to Associate VRF with Interface

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure interface to associate with an VRF.	<b>ip vrf forwarding</b> <i>vrf-name</i>	Mandatory By default, the interface is not associated with any VRF.
Configure an IP address for an interface.	<b>ip address</b> <i>ip-address</i> { <i>network-mask</i>   <i>mask-len</i> }	Mandatory By default, no IP address is configured for the interface.

## Note

- When the **ip vrf forwarding** command is configured under an interface, the existing IP address of the interface will be automatically deleted and needs to be reconfigured.

### 3. Configure VRF Attributes

When the local PE receives VPNv4 route information from the remote PE device, the local PE device needs to determine which local VRF to load this VPNv4 route into. To control the distribution of VPNv4 routes, each VRF requires one or more RT attributes, and there are two types of RT attributes: Export RT and Import RT. When the PE initiates a VPNv4 route carrying the Export RT attribute, the Export RT attribute carried by the route is used to match with the Import RT of the local VRF when the PE decides which VRF to import the VPNv4 route into.

In addition to the attributes of RT for VRF that controls VPNv4 route distribution, the routing policy on the VRF can also control route distribution, and there are two types of routing policies that can be configured: Import map and Export map. Import map uses route maps to control whether routes can be imported into the VRF, and Export maps use route maps to change the properties of routes originating from the VRF.

Table 5-79 Configuring VRF Attributes

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Create VRF and enter VRF configuration mode	<b>ip vrf</b> <i>vrf-name</i>	Mandatory By default, no VRF is configured.
Configuring RT for VRF	<b>route-target</b> [ <b>both</b>   <b>export</b>   <b>import</b> ] { <i>ASN:nn</i>   <i>IP-address:nn</i> }	Optional By default, no Export, Import RT attributes of VRF are configured.
Configure VRF inbound routing policies.	<b>import map</b> <i>rtmap-name</i>	Optional By default, no VRF inbound routing policy is configured.
Configure VRF outbound routing policy.	<b>export map</b> <i>rtmap-name</i>	Optional By default, no VRF outbound routing policy is configured.

---

## Note

- Import map and Export map policies are only valid for local routes.
  - Export map policy can not perform route filtering. It can only modify the properties of the VPN route published by VRF and can modify the following properties: community, extcommunity and local-preference.
  - When the PE imports VPNv4 routes into VRF, the RT matching rule has higher priority than the Import map policy, i.e., the RT rule is matched first, and then the Import map policy is matched.
- 

### Configure PE-PE inter-route switching.

In MPLS L3VPN networks, PEs interact with each other via MP-IBGP (Multiprotocol Extended BGP) for VPNv4 routes. Both ends of the PE are configured in the same way.

Table 6-7 Configuring PE-PE Inter-Route Switching

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable the BGP protocol and enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Configuring PE Neighbors	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>remote-as</b> <i>as-number</i>	Mandatory By default, there are no PE neighbors configured.
Configure the source address to be used for establishing PE neighbors.	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>update-source</b> { <i>interface</i>   <i>ip-address</i> }	Mandatory By default, the outgoing interface address of the route to the PE neighbor is used as the source address.
Enter BGP VPNv4 configuration mode.	<b>address-family vpnv4</b> [ <i>unicast</i> ]	Mandatory
Activate VPNv4 address clusters for PE neighbors.	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>activate</b>	Mandatory By default, only IPv4 unicast routes can be sent and received between BGP neighbors.
Configure to send extended group attributes to PE neighbors.	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>send-community</b> [ <b>both</b>   <b>extended</b>   <b>standard</b> ]	Optional By default, the VPNv4 address clusters of active neighbors are automatically configured to send extended group attributes.

---

## Note

- Many of the routing characteristics under BGP VPNv4 address clusters are the same as those under BGP IPv4 unicast address clusters, and these characteristics are selected according to the networking requirements, as described in the MPLS L3VPN section in the Command
-

### Configure PE-CE inter-route switching.

Routing exchange between PE and CE can use static routes, RIP, OSPF, ISIS and BGP routing protocols, depending on the actual network environment will determine which method to use. The PE is configured in the same way as the CE.

#### 1. Configure to Use Static Route between PE and CE

Table 79-8 Configuring to Use Static Route between PE and CE

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure a static route to the CE.	<b>ip route vrf</b> <i>vrf-name destination-ip-address destination-mask nexthop-ip-address</i>	Mandatory By default, no static route to the CE is configured.
Enable the BGP protocol and enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Enter the BGP IPv4 VRF configuration mode	<b>address-family ipv4 vrf</b> <i>vrf-name</i>	Mandatory By default, in BGP IPv4 unicast configuration mode.
Configure BGP to redistribute static routes.	<b>redistribute static</b> [ <b>route-map</b> <i>map-name / metric value</i> ]	Optional By default, the BGP is not configured to redistribute static route.

#### 2. Configure to Use RIP between PE and CE

Table 79-9 Configuring to Use RIP between PE and CE

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Enable RIP protocol and enter RIP configuration mode.	<b>router rip</b>	Mandatory By default, RIP is not enabled.
Enter the RIP VRF address family configuration mode	<b>address-family ipv4 vrf</b> <i>vrf-name</i>	Mandatory By default, the VRF address cluster of the RIP protocol is not enabled.
Configure the RIP version of the RIP protocol in VRF address cluster mode.	<b>version</b> {1   2}	Mandatory By default, the version used by RIP is version 1, which should generally be modified to version 2.
Configure the RIP to override the PE and CE connection interface.	<b>network</b> [ <i>network-address</i>   <i>interface</i> ]	Mandatory By default, RIP does not cover the PE and CE connection interface.
Exit RIP protocol VRF address cluster configuration mode.	<b>exit-address-family</b>	-
Exit RIP configuration mode.	<b>exit</b>	-
Enable the BGP protocol and enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Enter the BGP IPv4 VRF configuration mode	<b>address-family ipv4 vrf</b> <i>vrf-name</i>	Mandatory By default, in BGP IPv4 unicast configuration mode.
Configure BGP to redistribute RIP.	<b>redistribute rip</b> [ <b>route-map</b> <i>map-name</i> / <b>metric</b> <i>value</i> ]	Optional By default, there is no redistribution of RIP protocol routes.

### 3. Configure to Use OSPF between PE and CE

Table 10-11 Configuring to Use OSPF between PE and CE

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Create OSPF process and enter OSPF configuration mode	<b>router ospf</b> <i>process-id vrf vrf-name</i>	Mandatory  OSPF process is enabled in VRF, by default the system does not enable OSPF protocol.  When OSPF is enabled from VRF, the OSPF process belonging to a certain VRF can manage the interfaces belonging to this VRF only.
Configure OSPF to override the PE-CE connection interface.	<b>network</b> <i>ip-address wildcard-mask</i> <b>area area-id</b>	Mandatory  By default, interface doesn't belong to any OSPF process or area.  One interface can only belong to one OSPF process and area.
Exit OSPF configuration mode.	<b>exit</b>	-
Enable the BGP protocol and enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Enter the BGP IPv4 VRF configuration mode	<b>address-family ipv4 vrf</b> <i>vrf-name</i>	Mandatory  By default, in BGP IPv4 unicast configuration mode.
Configure BGP to redistribute OSPF.	<b>redistribute ospf</b> <i>as-number</i> [ <b>route-map</b> <i>map-name</i> / <b>metric value</b> / <b>match level</b> ]	Optional  By default, there is no redistribution of RIP protocol routes.

#### 4. Configure to Use ISIS between PE-CE

Table 12-9 Configuring to Use ISIS between PE-CE

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the IS-IS configuration mode	<b>router isis</b> [ <i>instance-name</i> ]	-
Configure network entity title for IS-IS	<b>net</b> <i>entry-title</i>	Mandatory By default, IS-IS doesn't have network entity title.
Configure IS-IS VRF attributes	<b>vrf</b> <i>vrf-name</i>	Optional By default IS-IS processes are located in the global VRF.
Return to the global configuration mode	<b>exit</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure the interface to associate a VPF instance.	<b>ip vrf forwarding</b> <i>vrf-name</i>	Mandatory By default, the interface is not associated with any VRF.
Enable IS-IS protocol for the interface	<b>ip router isis</b> [ <i>instance-name</i> ]	Mandatory IS-IS protocol is not enabled on the interface by default.
Return to the global configuration mode	<b>exit</b>	-
Enable the BGP protocol and enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Enter the BGP IPv4 VRF configuration mode	<b>address-family ipv4 vrf</b> <i>vrf-name</i>	Mandatory

Step	Command	Description
		By default, in BGP IPv4 unicast configuration mode.
Configure BGP to redistribute ISIS.	<b>redistribute isis</b> [ <i>instance-name</i> ] [ <b>route-map</b> <i>map-name</i> / <b>metric value</b> / <b>match level</b> ]	Optional  By default, there is no redistribution of ISIS protocol routes.

## 5. Configure to Use BGP between PE and CE

Table 13-14 Configuring to Use BGP between PE and CE

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable the BGP protocol and enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Enter the BGP IPv4 VRF configuration mode	<b>address-family ipv4 vrf</b> <i>vrf-name</i>	Mandatory  By default, in BGP IPv4 unicast configuration mode.
Configure CE as an EBGP neighbor.	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>remote-as</b> <i>as-number</i>	Mandatory  By default, there are no CE neighbors configured.

### 79.2.2 Configure M-VRF.

#### Configuration Condition

Before configuring the M-VRF, do the following:

- Configure the link layer protocol for the connection interface between M-VRF device and the PE and the site, keeping them connected.

#### Configure M-VRF.

M-VRF is an inexpensive way to extend VPN functionality to CEs. When multiple services exist for customers, instead of dividing multiple services onto one CE, multiple VRFs are configured on the M-VRF device to virtualize multiple CEs, isolating each service. The following figure depicts an example of M-VRF.

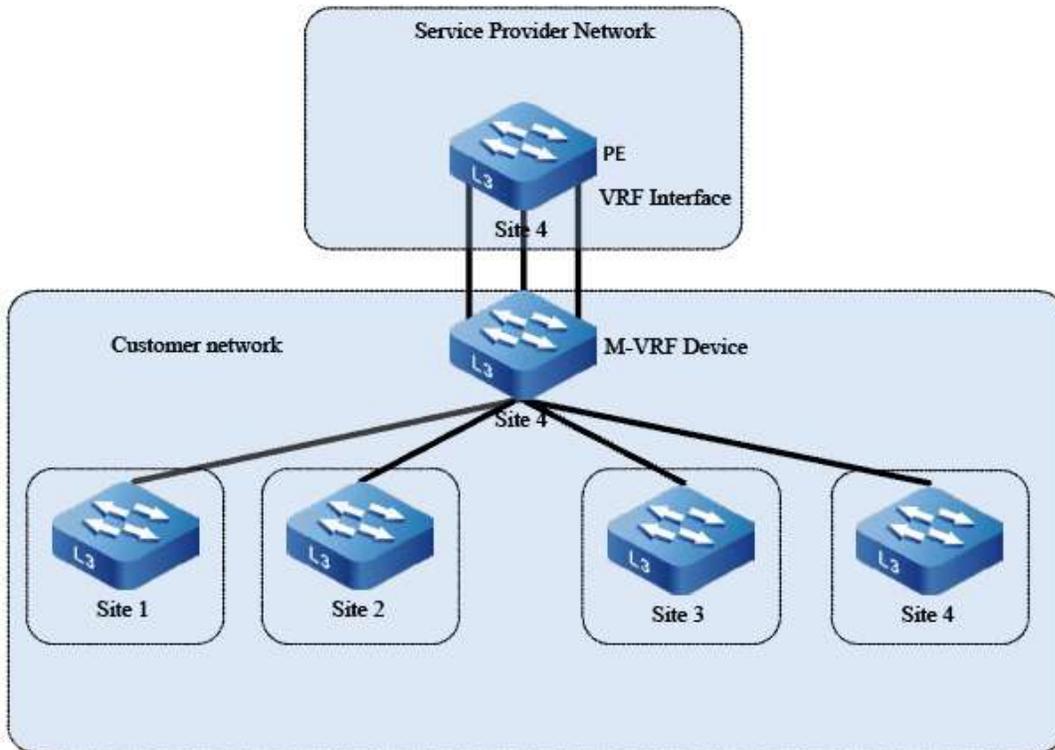


Figure 2-3 Configuring M-VRF

One interface in each VRF on the M-VRF device connects to the site and the other interface connects to the PE. In general, M-VRF devices connect to PEs using Ethernet connections, using one interface per VRF.

### 1. Configure the Routing Exchange between M-VRF Device and PE

Routing exchange between M-VRF devices and CEs can use static routes, RIP, OSPF, ISIS, and BGP routing protocols. The following is an example of routing exchange using RIP only.

Table 15-16 Configuring Routing Exchange Between M-VRF Device and PE

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Create VRF and enter VRF configuration mode	<b>ip vrf vrf-name</b>	Mandatory

Step	Command	Description
		By default, no VRF is configured.
Configure RD for VRF.	<b>rd</b> <i>route-distinguisher</i>	Mandatory By default, RD for VRF is not configured.
Exit VRF configuration mode.	<b>exit</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface_name</i>	-
Configure interface to associate with an VRF.	<b>ip vrf forwarding</b> <i>vrf-name</i>	Mandatory By default, the interface is not associated with any VRF.
Configure an IP address for an interface.	<b>ip address</b> <i>ip-address</i> { <i>network-mask</i>   <i>mask-len</i> }	Mandatory By default, no IP address is configured for the interface.
Exit interface configuration mode	<b>exit</b>	-
Enable RIP protocol and enter RIP configuration mode.	<b>router rip</b>	Mandatory By default, RIP is not enabled.
Enter the RIP VRF address family configuration mode	<b>address-family ipv4 vrf</b> <i>vrf-name</i>	Mandatory By default, the RIP protocol does not enable VRF address clustering.
Configure the RIP version of the RIP protocol in VRF address cluster mode.	<b>version</b> {1   2}	Mandatory By default, the version used by RIP is version 1.
Configure RIP to override the connection interface	<b>network</b> [ <i>network-address</i>   <i>interface</i> ]	Mandatory By default, RIP does not override the interface

Step	Command	Description
between the M-VRF device and PE .		between the M-VRF device and the PE connection.

## Note

- Each VRF needs to be configured separately on the MVRF device with reference to the steps above.
- For the configuration of the PE side, refer to the "Configuring Basic Functions of VPN" section.

## 2. Configure M-VRF Devices and Inter-Site Routing Exchange

Routing exchange between M-VRF devices and sites can use static routing, RIP, OSPF, ISIS, and BGP routing protocols. The following is an example of using static routes.

Table 17-18 Configuring M-VRF and Inter-site Routing Exchange

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Create VRF and enter VRF configuration mode	<b>ip vrf</b> <i>vrf-name</i>	Mandatory By default, no VRF is configured.
Configure RD for VRF.	<b>rd</b> <i>route-distinguisher</i>	Mandatory By default, RD for VRF is not configured.
Exit VRN instance configuration mode	<b>exit</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface_name</i>	-
Configure interface to associate with an VRF.	<b>ip vrf forwarding</b> <i>vrf-name</i>	Mandatory

Step	Command	Description
		By default, the interface is not associated with any VRF.
Configure an IP address for an interface.	<b>ip address</b> <i>ip-address</i> { <i>network-mask</i>   <i>mask-len</i> }	Mandatory  By default, no IP address is configured for the interface.
Exit interface configuration mode	<b>exit</b>	-
Configure a static route to the site.	<b>ip route vrf</b> <i>vrf-name destination-ip-address destination-mask</i> <i>nexthop-ip-address</i>	Mandatory  By default, no static route to the site is configured.

---

### Note

- Each VRF needs to be configured separately on the MVRF device with reference to the steps above.
  - The site is configured in the same way as a normal static route configuration.
- 

### 79.2.3 Configure VPN route label assignment.

#### Configuration Condition

Before configuring the VPN route label assignment method, do the following:

- Configure basic VPN functions.

#### Configure VPN route label assignment.

BGP provides two ways to assign labels to VPN routes: the per-route label assignment method and the per-VRF label assignment method. With the per-route approach, BGP assigns a different label to each VPN route; with the per-VRF approach, BGP assigns the same label to VPN routes in the same VRF, and different labels to routes in different VRFs.

By default, BGP uses the per-VRF label assignment method, which can save label resources and reduce ILM table entry generation and improve performance when the amount of locally published VPN routes is large.

Table 19-20 Configuring VPN Route Label Assignment

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable the BGP protocol and enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Configure per-route label assignment method.	<b>no unique-label-per-vrf</b>	Optional By default, the per-VRF label assignment method is enabled.

### 79.2.4 Configure VPN to cross domain.

#### Configuration Condition

Before configuring VPN to cross domain, do the following:

- Configure basic VPN functions.
- Configure the IP address for ASBR direct connection to achieve IP reachability between ASBRs.

#### Configure Option-A to cross domain.

Cross-domain Option-A , also known as VRF-to-VRF, is the easiest way to achieve VPN inter-access between AS. VRF-to-VRF handles inter-AS VPNv4 connectivity by simply treating another ASBR as a CE device. The following figure depicts an example of a VRF-to-VRF approach to cross domain.

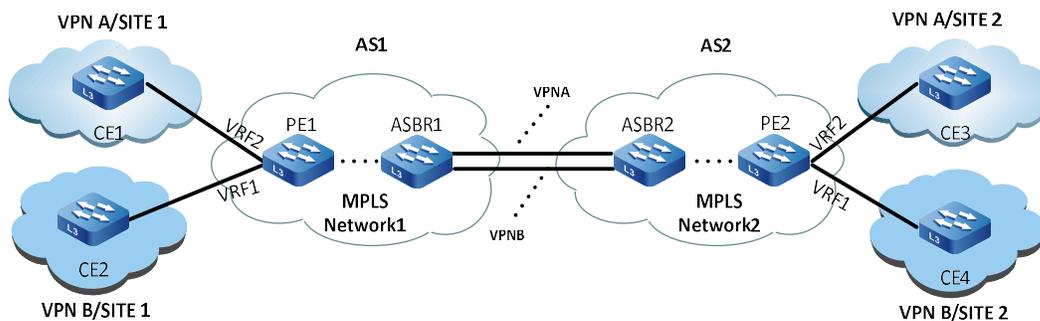


Figure 4-5 Configuring Option-A to Cross Domain (VRF-to-VRF)

In the above figure, VPN A Site 1 and Site 2 are connected to two different service providers: AS1 and AS2, and the service providers are connected to each other via ASBR. When two AS domains are configured with MPLS L3VPN networks, the VPN acrossing the AS domain requires the local ASBR to act as the PE device of the VPN and the peer ASBR to act as the CE device of the VPN. The VRF corresponding to this VPN should be configured on both ASBR devices at the same time. In this way, VPN routes are communicated within the AS via MP-IBGP for VPNv4 routes, and unicast routes are communicated between ASBRs within the corresponding VRFs of this VPN, thus achieving connectivity between Site 1 and Site 2.

The advantage of the VRF-to-VRF approach is that there is no need to run MPLS between ASBRs, and the disadvantage is that it is less scalable as the ASBR has to maintain routes for all VPNs and assign interfaces and connections to each cross-domain VPN.

See the section on "Configuring Basic Functions of VPN" for configuring method of VRF-to-VRF cross-domain.

**Configure Option-B to cross domain.**

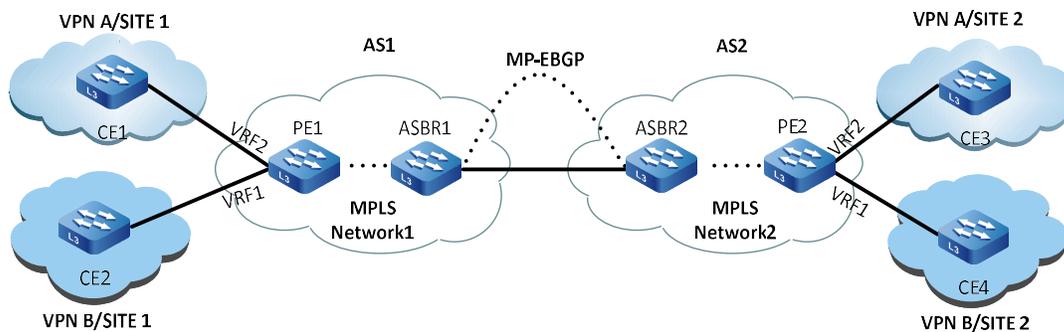


Figure 6-7 Configuring Option-B to Cross Domain (MP-EBGP Carrying VPNv4 Routes)

Option-B needs to run MP-EBGP between ASBR to cross domain. When the ASBR learns all VPN routes of the local autonomous domain PE, it re-assigns new labels to the VPN routes and then advertises the routing information and the new labels to the peer ASBR. The ASBR needs to maintain all VPN routes received from the local PE and the peer ASBR.

The method for Option-B to cross domain does not require ASBR to configure VRFs for each VPN, import VPNv4 routes, or assign interfaces to each VPN. However, ASBR still needs to maintain all VPNv4 routes and assign new labels to each label and install ILM table entries locally for old and new label conversions, so ASBR is under more pressure to carry the load.

Table 21-22 Configuring Option-B to Cross Domain

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Enable MPLS forwarding globally	<b>mpls ip</b>	Mandatory By default, MPLS forwarding is not enabled
Enter the interface configuration mode	<b>interface</b> <i>interface_name</i>	-
Enable MPLS forwarding on the interface	<b>mpls ip</b>	Mandatory Configuration is done on the interconnect interface of the two ASBRs. By default, MPLS forwarding is not enabled on the interface.
Return to the global configuration mode	<b>exit</b>	-
Enable the BGP protocol and enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Configure the peer ASBR as an EBGP neighbor.	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>remote-as</b> <i>as-number</i>	Mandatory By default, there are no EBGP neighbors configured.
Enter BGP VPNv4 configuration mode.	<b>address-family vpnv4</b> [ <i>unicast</i> ]	Mandatory By default, in BGP IPv4 unicast configuration mode.
Activate MP-EBGP neighbor advertisement VPN routes.	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>activate</b>	Mandatory By default, BGP only advertises IPv4 unicast routes.
Configure to change the next hop when advertising the PE to the route.	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-</i>	Mandatory By default, the next hop is not configured to

Step	Command	Description
	<i>group-name</i> } <b>next-hop-self</b>	change when the route is advertised to the PE.

## Note

- The above only lists the basic configuration of Option-B to cross domain on ASBR. For the configuration between ASBR and PE and P devices in this AS, refer to the "Configuring Basic Functions of VPN" section.

### 79.2.5 Configure VPN users to access the Internet.

#### Configuration Condition

Before configuring VPN users to access the Internet, do the following:

- Configure basic VPN functions.

#### Configure CE access to the Internet.

In the actual application environment, customers do not want VPN users to access the Internet directly and require security devices such as firewalls to control the connection of VPN users to the Internet. Each VPN site sends its Internet data stream to the central site. VPN members forward their data streams to access the Internet to the central site by importing a default route to access the Internet (with the next hop being the central site CE). The central site forwards the data stream to the Internet to the enterprise firewall, which does the necessary access control and NAT processing according to the security policy formulated within the firewall, and finally the firewall forwards the data stream to the Internet. The following figure depicts an example of using CE access to access the Internet.

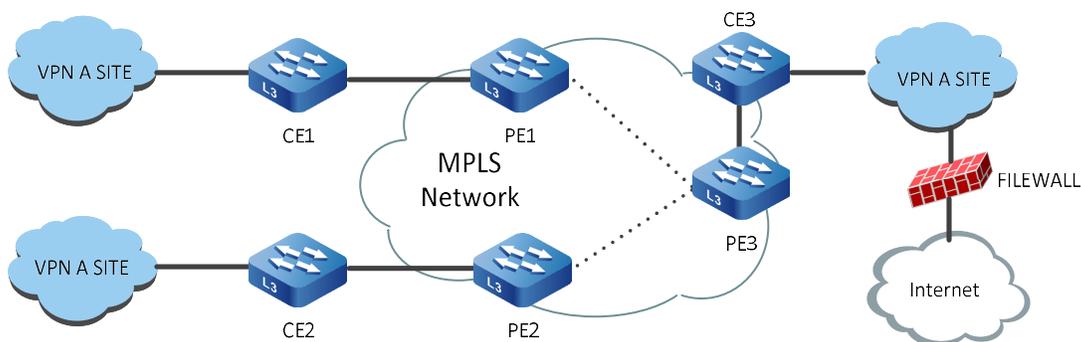


Figure 79-8 Configuring CE Access to the Internet

In the above figure, CE3 is used as the central site for customer control of Internet access, and it is only necessary to configure the default route on CE3 with the next hop as the Internet gateway, which is communicated to the PE device through the route exchange between PE and CE, and then communicated to each VPN site through MP-IBGP, so that each VPN site can access the Internet through the default route (the next hop is PE3), and the access to Internet data first arrives at CE3 through the MPLS network, and then reaches the Internet through the default route configured on CE3.

This CE access method only requires configuration and deployment within the VPN, without operator involvement, and users are free to control the security policy for internal user access to the Internet. However, this approach requires users to have strong security management capabilities, and it is not possible for operators to achieve unified management of user access to the Internet.

Table 23-24 Configuring CE Access to the Internet

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the default route on the central site CE with the Internet gateway as the next hop.	<b>ip route</b> <i>destination-ip-address</i> <i>destination-mask</i> <i>nexthop-ip-address</i>	Mandatory  By default, CE is not configured with a default route to the Internet.

---

 **Note**

- For the configuration of other devices, refer to the "Configuring Basic Functions of VPN" section.
- 

**Configure PE access to the Internet.**

Internet access can be provided to VPN users by forwarding their traffic to the Internet gateway of the service provider network, which is called PE access to the Internet. To provide Internet access to the VPN, the global routing table on the PE must be able to forward VPN traffic, which is achieved by creating a static route in the PE's VRF and specifying the next hop in the global routing table. The following figure depicts an example of PE access to the Internet.

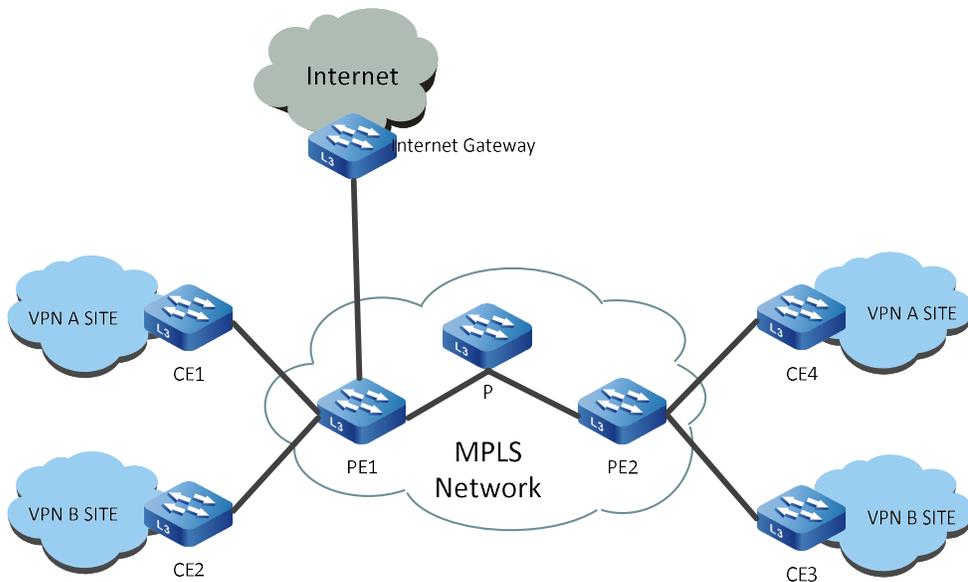


Figure 9-10 Configuring PE Access to the Internet

In the above figure, VPN A has two users, CE1 and CE4, who need to access the Internet. First, you need to configure a cross-VRF default static route to access the Internet in the VRF routing tables of PE1 and PE2 respectively, where the next hop of the cross-VRF default static route in PE1 is the Internet gateway and the next hop of the cross-VRF default static route in PE2 is PE1. In order to ensure that the packets returned from the Internet can be successfully returned to CE1 and CE4, it is also necessary to configure a cross-VRF route reaching CE1 in the global routing table of PE1, with the next hop being CE1 in the VRF; in the global routing table of PE2, it is also necessary to configure a cross-VRF route reaching CE4, with the next hop being CE4 in the VRF, and to advertise this route to the MPLS network via IGP.

Table 79-25 Configuring PE Access to the Internet

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the default static route across the VRF to access the Internet in the PE's VRF routing table, with the next hop being the Internet gateway.	<b>ip route vrf vrf-name destination-ip-address destination-mask nexthop-ip-address vrf global</b>	Mandatory By default, there is no default static route configured for the PE to access the Internet.
Configure a static route across the VRF in the PE's global routing table to reach the CE, with the next hop being the CE.	<b>ip route destination-ip-address destination-mask nexthop-ip-address vrf vrf-name</b>	Mandatory By default, no static route across the VRF is

Step	Command	Description
		configured for the PE to reach the CE.

---

## Note

- The above is the key configuration for the PE connected to the Internet gateway (corresponding to PE1 in the figure). For other PEs (such as PE2 in the figure), configure a default static route across the VRF to access the Internet, and the next hop needs to point to the loopback port address of PE1 (meaning the loopback port where the BGP neighbor is established).
- 

### 79.2.6 Configure AS override.

#### Configuration Condition

Before configuring AS override, do the following:

- Configure basic VPN functions.
- Configure the PE-CE inter-route exchange to use EBGP.

#### Configure AS override.

When running BGP between PE and CE routers, the customer VPN may wish to reuse AS numbers within different sites, which inevitably produces a route from the PE that is received by the CE with an AS-PATH attribute that will contain the AS number on the CE device side, and the CE will discard the route from the PE. To resolve this situation, the PE needs to enable the BGP AS override feature. After the PE device enables the AS override function, when it advertises the route to the CE neighbor, if the AS-PATH of the route has the same AS number as the CE, the PE will replace the AS number of the CE neighbor contained in the AS-PATH attribute of the route with its own AS number and then advertise it to the CE neighbor.

Table 79-26 Configuring AS Override

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Enable the BGP protocol and enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Enter the BGP IPv4 VRF configuration mode	<b>address-family ipv4 vrf</b> <i>vrf-name</i>	Mandatory By default, in BGP IPv4 unicast configuration mode.
Configure AS Override	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>as-override</b>	By default, the AS override function is not enabled.

## 79.2.7 Configure OSPF Pseudo-Connections

### Configuration Condition

Before configuring an OSPF pseudo-link, do the following:

- Configure basic functions of VPN and configure OSPF for routing exchange between PE and CE.

### Configure OSPF Pseudo-Connections

In an MPLS L3VPN environment, when there is a directly connected backup link (called a "backdoor link") between two CEs at different sites, the OSPF intra-domain route takes precedence over the external route redistributed from BGP, resulting in traffic between the CEs not going through the VPN, but rather through the backdoor link. In order to prioritize traffic between two CEs to pass through the VPN, an OSPF pseudo-link needs to be established between the two PEs.

The source and destination addresses of the pseudo-link are reachable within the BGP domain and cannot be overwritten and redistributed by OSPF. Routes to pseudo-link destinations can only be learned through BGP.

The OSPF pseudo-link configuration steps on the PE are as follows.

#### 1. Configure VRF Loopback Interface

Table 27-28 Configuring the VRF Loopback Interface

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Create loopback interface and enter interface configuration mode.	<b>interface loopback</b> <i>interface-number</i>	Mandatory By default, no loopback interface is created.
Configure loopback interface to associate with VRF.	<b>ip vrf forwarding</b> <i>vrf-name</i>	Mandatory By default, the interface is not associated with any VRF.
Configure the loopback interface IP address.	<b>ip address</b> <i>ip-address</i> { <i>mask</i>   <i>mask-length</i> }	Mandatory By default, no interface IP address is configured.
Exit interface configuration mode	<b>exit</b>	-

## 2. Configure BGP to Redistribute OSPF and Directly Connected Route of Loopback Interface

Table 29-30 Configure BGP to Redistribute OSPF and Directly Connected Route of Loopback Interface

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable the BGP protocol and enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	-
Enter the BGP IPv4 VRF configuration mode	<b>address-family ipv4 vrf</b> <i>vrf-name</i>	Mandatory By default, in BGP IPv4 unicast configuration mode.
Configure BGP to redistribute directly connected route of loopback interface.	<b>redistribute connected</b> [ <b>route-map</b> <i>map-name</i> / <b>metric</b> <i>value</i> ]	Mandatory By default, BGP does not redistribute directly connected routes
Configure BGP to redistribute OSPF.	<b>redistribute ospf</b> <i>as-number</i> [ <b>match</b> <i>route-sub-type</i> /	Mandatory By default, BGP does not redistribute OSPF routes.

Step	Command	Description
	<b>route-map</b> <i>map-name / metric value</i> ]	
Exit the BGP IPv4 VRF configuration mode	<b>exit-address-family</b>	-
Exit the BGP configuration mode	<b>exit</b>	-

### 3. Configure OSPF Pseudo-Connections

Table 31-32 Configuring OSPF Pseudo-Connections

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Create OSPF process and enter OSPF configuration mode	<b>router ospf</b> <i>process-id</i> [ <b>vrf</b> <i>vrf-name</i> ]	Mandatory  Enable the OSPF process directly or from VRF. By default, the OSPF protocol is disabled in the system.  When OSPF is enabled from VRF, the OSPF process belonging to a certain VRF can manage the interfaces belonging to this VRF only.
Configure the network segment covered by OSPF area	<b>network</b> <i>ip-address wildcard-mask area area-id</i>	Mandatory  By default, interface doesn't belong to any OSPF process or area.  One interface can only belong to one OSPF process and area.
Configure OSPF Pseudo-Connections	<b>area</b> <i>area-id sham-link source-ip-address desinationt-ip-address</i> [ <b>cost</b> <i>cost</i> ]	Mandatory  <i>source-ip-address</i> should be the local loopback address, <i>desinationt-ip-</i>

Step	Command	Description
		<p><i>address</i> should be the peer loopback address.</p> <p>By default, no OSPF pseudo-link is configured.</p>

## 79.2.8 MPLS L3VPN Monitoring and Maintaining

Table 33-34 MPLS L3VPN Monitoring and Maintaining

Command	Description
<b>clear ip bgp</b> { * [vrf vrf-name]   neighbor-address [vrf vrf-name]   as-number   peer-group peer-group-name   external }	Reset BGP neighbors
<b>clear ip bgp</b> { *   neighbor-address   as-number   peer-group peer-group-name   external } [vpn4 unicast   vrf vrf-name] { [ soft ] [ in   out ] }	Softly reset neighbors
<b>show ip bgp vpnv4</b> { all   vrf vrf-name   rd route-distinguisher } [ ip-address   ip-address/mask-length ]	Display routing database information under BGP VPNv4 address clusters.
<b>show ip bgp vpnv4</b> { all   vrf vrf-name   rd route-distinguisher } dampening { dampened-paths   flap-statistics   parameters }	Show details of BGP VPNv4 route decay.
<b>show ip bgp</b> [ vpnv4 { all   vrf vrf-name   rd route-distinguisher } ] labels	Display route label information under BGP VPNv4 address clusters.
<b>show ip bgp vpnv4 all neighbors</b> [ ip-address ]	Display neighbor details under BGP VPNv4 address clusters.
<b>show ip bgp vpnv4</b> { all   vrf vrf-name   rd route-distinguisher } summary	Summary information of all neighbors under BGP VPNv4 address clusters.
<b>show ip bgp vrf</b> vrf-name	Display BGP VRF information

## 79.3 MPLS L3VPN Typical Configuration Example

### 79.3.1 Configure intra-domain MPLS L3VPN.

#### Network Requirements

- The entire MPLS network includes two VPNs, VPN1 and VPN2, and the two VPNs use different Route-Targets, thus ensuring that the two VPNs cannot inter-access each other.
- CE1 and CE3 belong to VPN1, and CE2 and CE4 belong to VPN2.
- OSPF is used for route advertisement between CE and PE.
- OSPF is used as IGP between PEs to achieve intra-PE communication, and MP-IBGP is configured to exchange VPN routing information.

#### Network Topology

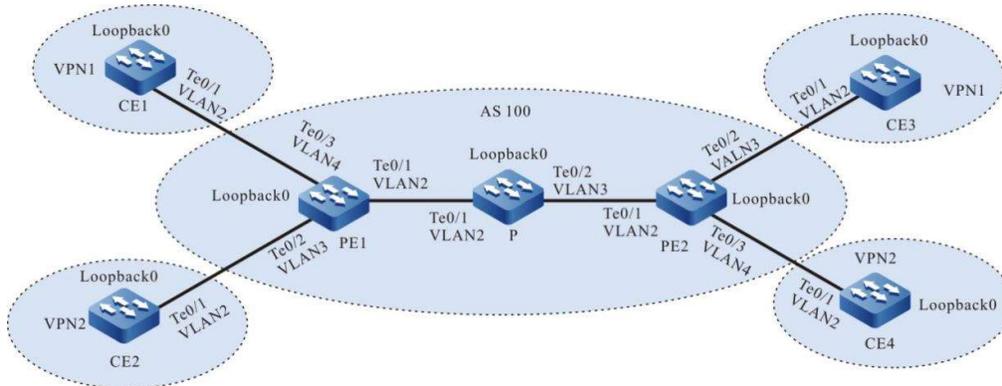


Figure 79-11 Network Topology for Configuring Intra-Domain MPLS L3VPN

Table 35-36 Interface Mapping Relationships

of equipment	Interface	IP address	of equipment	Interface	IP address
CE1	Vlan2	95.1.1.2/16	P	Loopback0	11.11.11.11/32
	Loopback0	5.5.5.5/32	PE2	Vlan2	92.1.1.1/16
PE1	Vlan2	93.1.1.2/16		Vlan3	90.1.1.1/16
	Vlan3	94.1.1.1/16		Vlan4	91.1.1.1/16
	Vlan4	95.1.1.1/16		Loopback0	75.75.75.75/32
	Loopback0	90.90.90.90/32	CE3	Vlan2	90.1.1.2/16

of equipment	Interface	IP address	of equipment	Interface	IP address
CE2	Vlan2	94.1.1.2/16		Loopback0	8.8.8.8/32
	Loopback0	2.2.2.2/32	CE4	Vlan2	91.1.1.2/16
P	Vlan2	93.1.1.1/16		Loopback0	3.3.3.3/32
	Vlan3	92.1.1.2/16			

### Configuration Steps

Step 1: Configure the VLAN and add the port to the corresponding VLAN in access mode.  
(Omitted)

Step 2: Configure IP addresses for the ports. (Omitted)

Step 3: Configure global OSPF to advertise global routes.

#Configure global OSPF on PE1.

```
PE1#configure terminal
PE1(config)#router ospf 100
PE1(config-ospf)#network 90.90.90.90 0.0.0.0 area 0
PE1(config-ospf)#network 93.1.0.0 0.0.255.255 area 0
PE1(config-ospf)#exit
```

# Configure global OSPF on P.

```
P#configure terminal
P(config)#router ospf 100
P(config-ospf)#network 11.11.11.11 0.0.0.0 area 0
P(config-ospf)#network 92.1.0.0 0.0.255.255 area 0
P(config-ospf)#network 93.1.0.0 0.0.255.255 area 0
P(config-ospf)#exit
```

#Configure global OSPF on PE2.

```
PE2#configure terminal
PE2(config)#router ospf 100
PE2(config-ospf)#network 75.75.75.75 0.0.0.0 area 0
PE2(config-ospf)#network 92.1.0.0 0.0.255.255 area 0
PE2(config-ospf)#exit
```

#After the configuration is complete, view the global routing table on the device.

Take PE1 as an example:

```
PE1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
O 11.11.11.11/32 [110/2] via 93.1.1.1, 00:05:12, vlan2
O 75.75.75.75/32 [110/3] via 93.1.1.1, 00:06:03, vlan2
C 93.1.0.0/16 is directly connected, 00:34:54, vlan2
L 93.1.1.2/32 is directly connected, 00:34:54, vlan2
O 92.1.0.0/16 [110/2] via 93.1.1.1, 00:08:12, vlan2
LC 90.90.90.90/32 is directly connected, 154:02:28, loopback0
```

It is indicated that the global routing table of PE1 has the routing information of the loopback port of P and PE2 present.

---

## Note

- Refer to PE1 for the inspection method of P and PE2.
- 

Step 4: Enable MPLS IP and MPLS LDP.

#Enable global MPLS IP and MPLS LDP on PE1, and also enable MPLS IP and MPLS LDP on the interface.

```
PE1(config)#mpls ip
PE1(config)#mpls ldp
PE1(config-ldp)#router-id 90.90.90.90
PE1(config-ldp)#address-family ipv4
PE1(config-ldp-af4)#transport-address 90.90.90.90
PE1(config-ldp-af4)#exit
PE1(config-ldp)#exit
PE1(config)#interface vlan2
PE1(config-if-vlan2)#mpls ip
PE1(config-if-vlan2)#mpls ldp
PE1(config-if-vlan2)#exit
```

# Enable global MPLS IP and MPLS LDP on P. Also enable MPLS IP and MPLS LDP on the interface.

```
P(config)#mpls ip
```

```
P(config)#mpls ldp
P(config-ldp)#router-id 11.11.11.11
P(config-ldp)#address-family ipv4
P(config-ldp-af4)#transport-address 11.11.11.11
P(config-ldp-af4)#exit
P(config-ldp)#exit
P(config)#interface vlan2
P(config-if-vlan2)#mpls ip
P(config-if-vlan2)#mpls ldp
P(config-if-vlan2)#exit
P(config)#interface vlan3
P(config-if-vlan3)#mpls ip
P(config-if-vlan3)#mpls ldp
P(config-if-vlan3)#exit
```

# Enable global MPLS IP and MPLS LDP on PE2, and also enable MPLS IP and MPLS LDP on the interface.

```
PE2(config)#mpls ip
PE2(config)#mpls ldp
PE2(config-ldp)#router-id 75.75.75.75
PE2(config-ldp)#address-family ipv4
PE2(config-ldp-af4)#transport-address 75.75.75.75
PE2(config-ldp-af4)#exit
PE2(config-ldp)#exit
PE2(config)#interface vlan2
PE2(config-if-vlan2)#mpls ip
PE2(config-if-vlan2)#mpls ldp
PE2(config-if-vlan2)#exit
```

---

## Note

- router-id and transport-address can be manually configured or automatically generated, and are generally configured to be the same. If router-id and transport-address are not manually configured, the device will automatically select them. Among the interfaces in the up state, the largest IP address in the Loopback interface is selected first; if the device is not configured with a Loopback interface address, the largest IP address in the normal interface is selected.
- 

# After the configuration is complete, view the LDP session information on the device.

Take PE1 as an example:

```
PE1#show mpls ldp session
```

```
Peer IP Address Peer Type My Role State DS Cap DeadTime
11.11.11.11 Multicast Active OPERATIONAL Disabled 00:02:27
```

Statistics for ldp sessions:

Multicast sessions: 1

Targeted sessions: 0

It is indicated that PE1 successfully establishes an LDP session with P.

#View the routing label table entries on the device.

Take PE1 as an example:

```
PE1#show ip route 11.11.11.11 detail
```

```
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
```

```
U - Per-user Static route
```

```
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
O 11.11.11.11/32 [110/2] via 93.1.1.1, label 3, 00:29:21, vlan2
    93.1.1.1 [0], vlan2
```

```
PE1#show ip route 75.75.75.75 detail
```

```
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
```

```
U - Per-user Static route
```

```
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
O 75.75.75.75/32 [110/3] via 93.1.1.1, label 16, 00:29:15, vlan2
    93.1.1.1 [0], vlan2
```

It is indicated the label information of the loopback ports to P and PE2 exist on PE1.

---

## Note

- Refer to PE1 for the inspection method of P and PE2.
- 

Step 5: Configure the VPN instance to advertise the CE route to the PE via OSPF.

#Configure VPN instance on PE1 and OSPF under VPN1 and VPN2.

```
PE1(config)#ip vrf 1
PE1(config-vrf)#rd 100:1
PE1(config-vrf)#route-target export 100:1
PE1(config-vrf)#route-target import 100:1
PE1(config-vrf)#exit
PE1(config)#ip vrf 2
PE1(config-vrf)#rd 200:1
PE1(config-vrf)#route-target export 200:1
PE1(config-vrf)#route-target import 200:1
PE1(config-vrf)#exit
PE1(config)#interface vlan4
PE1(config-if-vlan4)#ip vrf forwarding 1
PE1(config-if-vlan4)#ip address 95.1.1.1 255.255.0.0
PE1(config-if-vlan4)#exit
PE1(config)#interface vlan3
PE1(config-if-vlan3)#ip vrf forwarding 2
PE1(config-if-vlan3)#ip address 94.1.1.1 255.255.0.0
PE1(config-if-vlan3)#exit
PE1(config)#router ospf 200 vrf 1
PE1(config-ospf)#network 95.1.0.0 0.0.255.255 area 0
PE1(config-ospf)#exit
PE1(config)#router ospf 300 vrf 2
PE1(config-ospf)#network 94.1.0.0 0.0.255.255 area 0
PE1(config-ospf)#exit
```

#Configure OSPF on CE1.

```
CE1#configure terminal
CE1(config)#router ospf 100
CE1(config-ospf)#network 5.5.5.5 0.0.0.0 area 0
CE1(config-ospf)#network 95.1.0.0 0.0.255.255 area 0
CE1(config-ospf)#exit
```

#Configure OSPF on CE2.

```
CE2#configure terminal
CE2(config)#router ospf 100
CE2(config-ospf)#network 2.2.2.2 0.0.0.0 area 0
CE2(config-ospf)#network 94.1.0.0 0.0.255.255 area 0
CE2(config-ospf)#exit
```

#Configure VPN instance on PE2 and configure OSPF under VPN1 and VPN2.

```
PE2(config)#ip vrf 1
```

```

PE2(config-vrf)#rd 100:1
PE2(config-vrf)#route-target export 100:1
PE2(config-vrf)#route-target import 100:1
PE2(config-vrf)#exit
PE2(config)#ip vrf 2
PE2(config-vrf)#rd 200:1
PE2(config-vrf)#route-target export 200:1
PE2(config-vrf)#route-target import 200:1
PE2(config-vrf)#exit
PE2(config)#interface vlan3
PE2(config-if-vlan3)#ip vrf forwarding 1
PE2(config-if-vlan3)#ip address 90.1.1.1 255.255.0.0
PE2(config-if-vlan3)#exit
PE2(config)#interface vlan4
PE2(config-if-vlan4)#ip vrf forwarding 2
PE2(config-if-vlan4)#ip address 91.1.1.1 255.255.0.0
PE2(config-if-vlan4)#exit
PE2(config)#router ospf 200 vrf 1
PE2(config-ospf)#network 90.1.0.0 0.0.255.255 area 0
PE2(config-ospf)#exit
PE2(config)#router ospf 300 vrf 2
PE2(config-ospf)#network 91.1.0.0 0.0.255.255 area 0
PE2(config-ospf)#exit

```

#### #Configure OSPF on CE3.

```

CE3#configure terminal
CE3(config)#router ospf 100
CE3(config-ospf)#network 8.8.8.8 0.0.0.0 area 0
CE3(config-ospf)#network 90.1.0.0 0.0.255.255 area 0
CE3(config-ospf)#exit

```

#### #Configure OSPF on CE4.

```

CE4#configure terminal
CE4(config)#router ospf 100
CE4(config-ospf)#network 3.3.3.3 0.0.0.0 area 0
CE4(config-ospf)#network 91.1.0.0 0.0.255.255 area 0
CE4(config-ospf)#exit

```

#### #View the VPN routing table on the PE.

Take PE1 as an example:

```

PE1#show ip route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS

```

U - Per-user Static route

O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

O 5.5.5/32 [110/2] via 95.1.1.2, 00:11:11, vlan4

C 95.1.0.0/16 is directly connected, 00:11:45, vlan4

L 95.1.1.1/32 is directly connected, 00:11:45, vlan4

PE1#show ip route vrf 2

Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS

U - Per-user Static route

O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

O 2.2.2/32 [110/2] via 94.1.1.2, 00:22:53, vlan3

C 94.1.0.0/16 is directly connected, 00:23:25, vlan3

L 94.1.1.1/32 is directly connected, 00:23:25, vlan3

It is indicated that routes to CE1 and CE2 exist in the VPN1 and VPN2 routing tables of PE1.

---

## Note

- Refer to PE1 for the inspection method of PE2.
- 

Step 6: Configure the MP-IBGP to use the loopback interface as the peer address; and redistribute routes with each other and the IGP protocol under the VPN instance.

#Configure the MP-IBGP on PE1 to enable VPNv4 address clustering; and redistribute routes with each other and the IGP protocol under the VPN instance.

```
PE1(config)#router bgp 100
```

```
PE1(config-bgp)#neighbor 75.75.75.75 remote-as 100
```

```
PE1(config-bgp)#neighbor 75.75.75.75 update-source loopback0
```

```
PE1(config-bgp)#address-family vpnv4
```

```
PE1(config-bgp-af)#neighbor 75.75.75.75 activate
```

```

PE1(config-bgp-af)#neighbor 75.75.75.75 send-community extended
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#address-family ipv4 vrf 1
PE1(config-bgp-af)#redistribute ospf 200
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#address-family ipv4 vrf 2
PE1(config-bgp-af)#redistribute ospf 300
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
PE1(config)#router ospf 200 vrf 1
PE1(config-ospf)#redistribute bgp 100
PE1(config-ospf)#exit
PE1(config)#router ospf 300 vrf 2
PE1(config-ospf)#redistribute bgp 100
PE1(config-ospf)#exit

```

#Configure the MP-IBGP on PE2 to enable VPNv4 address clustering; and redistribute routes with each other and the IGP protocol under the VPN instance.

```

PE2(config)#router bgp 100
PE2(config-bgp)#neighbor 90.90.90.90 remote-as 100
PE2(config-bgp)#neighbor 90.90.90.90 update-source loopback0
PE2(config-bgp)#address-family vpnv4
PE2(config-bgp-af)#neighbor 90.90.90.90 activate
PE2(config-bgp-af)#neighbor 90.90.90.90 send-community extended
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#address-family ipv4 vrf 1
PE2(config-bgp-af)#redistribute ospf 200
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#address-family ipv4 vrf 2
PE2(config-bgp-af)#redistribute ospf 300
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#exit
PE2(config)#router ospf 200 vrf 1
PE2(config-ospf)#redistribute bgp 100
PE2(config-ospf)#exit
PE2(config)#router ospf 300 vrf 2
PE2(config-ospf)#redistribute bgp 100
PE2(config-ospf)#exit

```

---

## Note

- In practice, if there are two or more PE devices on the same site, it is recommended not to redistribute routes directly between different routing protocols, and if you must configure them, you need to configure a routing policy to prevent routing loops from being generated.
- 

Step 7: Check the result.

# After the configuration is complete, view the BGP neighbor information on the PE.

Take PE1 as an example:

```
PE1#show ip bgp vpnv4 all summary
BGP router identifier 90.90.90.90, local AS number 100
BGP table version is 6
1 BGP AS-PATH entries
0 BGP community entries

Neighbor      V  AS MsgRcvd MsgSent  TblVer  InQ  OutQ  Up/Down  State/PfxRcd
75.75.75.75  4  100   40   41     5   0  00:32:01   4

Total number of neighbors 1
```

The successful establishment of BGP neighbors between PE1 and PE2 can be seen from the fact that the contents of the column State/PfxRcd are shown as numbers (the number of received route prefixes from neighbors).

#View the BGP VPNv4 routing table and VPN routing table on the PE.

Take PE1 as an example:

```
PE1#show ip bgp vpnv4 vrf 1
BGP table version is 43, local router ID is 90.90.90.90
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop        Metric LocPrf Weight Path
Route Distinguisher: 100:1 (Default for VRF 1)
[O]*> 5.5.5.5/32   95.1.1.2         2    32768 ?
[B]*>i8.8.8.8/32   75.75.75.75      2  100  0 ?
[B]*>i90.1.0.0/16  75.75.75.75      1  100  0 ?
[O]*> 95.1.0.0/16  0.0.0.0          1    32768 ?
```

```
PE1#show ip bgp vpnv4 vrf 2
BGP table version is 43, local router ID is 90.90.90.90
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
```

```
Origin codes: i - IGP, e - EGP, ? - incomplete
```

```
   Network      Next Hop      Metric LocPrf Weight Path
Route Distinguisher: 200:1 (Default for VRF 2)
[O]*> 2.2.2.2/32    94.1.1.2        2    32768 ?
[B]*>i3.3.3.3/32    75.75.75.75     2 100  0 ?
[B]*>i91.1.0.0/16   75.75.75.75     1 100  0 ?
[O]*> 94.1.0.0/16   0.0.0.0         1    32768 ?
```

```
PE1#show ip route vrf 1
```

```
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
```

```
       U - Per-user Static route
```

```
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
O 5.5.5.5/32 [110/2] via 95.1.1.2, 00:22:51, vlan4
B 8.8.8.8/32 [200/2] via 75.75.75.75, 00:01:06, vlan2
B 90.1.0.0/16 [200/1] via 75.75.75.75, 00:01:06, vlan2
C 95.1.0.0/16 is directly connected, 00:23:25, vlan4
L 95.1.1.1/32 is directly connected, 00:23:25, vlan4
```

```
PE1#show ip route vrf 2
```

```
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
```

```
       U - Per-user Static route
```

```
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
O 2.2.2.2/32 [110/2] via 94.1.1.2, 00:22:53, vlan3
B 3.3.3.3/32 [200/2] via 75.75.75.75, 00:01:15, vlan2
B 91.1.0.0/16 [200/1] via 75.75.75.75, 00:01:15, vlan2
C 94.1.0.0/16 is directly connected, 00:23:25, vlan3
L 94.1.1.1/32 is directly connected, 00:23:25, vlan3
```

It is indicated the route information to the peer CE3 and CE4 under the BGP VPNv4 routing table, VPN1 and VPN2 routing table of PE1.

#View the routing label information on the PE.

Take PE1 as an example:

```
PE1#show ip route vrf 1 8.8.8.8 detail
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
        U - Per-user Static route
        O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
B 8.8.8.8/32 [200/0] via 75.75.75.75, label 5120, 01:04:26, vlan2
    93.1.1.1 [3], label 16, vlan2
```

```
PE1#show ip route vrf 2 3.3.3.3 detail
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
        U - Per-user Static route
        O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
B 3.3.3.3/32 [200/0] via 75.75.75.75, label 5121, 01:04:26, vlan2
    93.1.1.1 [3], label 16, vlan2
```

```
PE1#show mpls forwarding-table
Pro: L - LDP, B - MP-BGP, R - RSVP, M - Mapped-Route, ML - mLDP (ML FEC: Root
address/OT/OV), RM - RSVP P2MP (RM FEC: P2MP ID/TID)
S - Static Label
```

Pro	Ident	FEC	Inlabel	Outlabel	Outgoing	Next hop
B	1	0.0.0.0/0	10240	/	/	/
B	2	0.0.0.0/0	10241	/	/	/

It is indicated that the route label information of VPN1 and VPN2 exists in the MPLS forwarding table of PE1.

---

## Note

- Refer to PE1 for the inspection method of PE2.
- 

#Ping the loopback port of CE3 at CE1 to see if it can ping through.

```
CE1#ping 8.8.8.8
```

```
Press key (ctrl + shift + 6) interrupt it.
```

```
Sending 5, 76-byte ICMP Echos to 8.8.8.8 , timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100% (5/5). Round-trip min/avg/max = 0/0/0 ms.
```

#Ping the loopback port of CE4 on CE1 to see if it can ping through.

```
CE1#ping 3.3.3.3
```

```
Press key (ctrl + shift + 6) interrupt it.
```

```
Sending 5, 76-byte ICMP Echos to 3.3.3.3 , timeout is 2 seconds:
```

```
.....
```

```
Success rate is 0% (0/5).
```

It is indicated that devices within the same VPN can communicate normally, while devices in different VPNs cannot communicate and routes are isolated.

## 79.3.2 Configure M-VRF.

### Network Requirements

- The MCE is the device used as the VPN multi-instance switch on the client side.
- The routes of two user networks, VPN1 and VPN2, are isolated so that sites of the same VPN can communicate with each other and sites of different VPNs cannot communicate.
- CE1 and CE3 are the sites of VPN1, and CE2 and CE4 are the sites of VPN2.
- EBGP is used between PE1 and CE1, and RIP is used between PE1 and CE2.
- OSPF is used between MCE and PE2, and static routes are used between MCE and CE3 and CE4.

### Network Topology

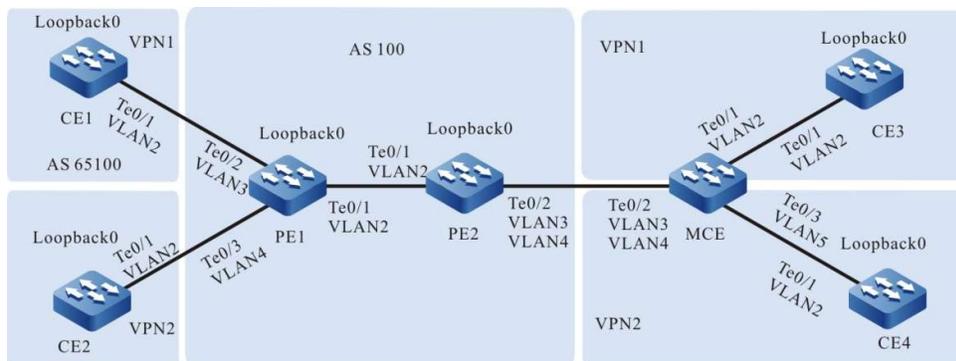


Figure 12-13 Network Topology for Configuring M-VRF

Table 37-38 Interface Mapping Relationships

of equipment	Interface	IP address	of equipment	Interface	IP address
CE1	Vlan2	95.1.1.2/16	PE2	Vlan4	92.1.1.2/16
	Loopback0	5.5.5.5/32		Loopback0	11.11.11.11/32
PE1	Vlan2	93.1.1.2/16	MCE	Vlan3	97.1.1.2/16
	Vlan3	95.1.1.1/16		Vlan4	92.1.1.1/16
	Vlan4	94.1.1.1/16		Vlan2	90.1.1.1/16
	Loopback0	90.90.90.90/32		Vlan5	91.1.1.1/16
CE2	Vlan2	94.1.1.2/16	CE3	Vlan2	90.1.1.2/16
	Loopback0	2.2.2.2/32		Loopback0	8.8.8.8/32
PE2	Vlan2	93.1.1.1/16	CE4	Vlan2	91.1.1.2/16
	Vlan3	97.1.1.1/16		Loopback0	3.3.3.3/32

### Configuration Steps

- Step 1: Configure Virtual Local Area Networks (VLANs), and add ports to the required VLANs. (Omitted)
- Step 2: Configure IP addresses for the ports. (Omitted)
- Step 3: Configure global OSPF to advertise global routes.

#Configure global OSPF on PE1.

```
PE1#configure terminal
PE1(config)#router ospf 100
PE1(config-ospf)#network 90.90.90.0 0.0.0.0 area 0
PE1(config-ospf)#network 93.1.0.0 0.0.255.255 area 0
PE1(config-ospf)#exit
```

#Configure global OSPF on PE2.

```
PE2#configure terminal
PE2(config)#router ospf 100
```

```
PE2(config-ospf)#network 11.11.11.11 0.0.0.0 area 0
PE2(config-ospf)#network 93.1.0.0 0.0.255.255 area 0
PE2(config-ospf)#exit
```

#After the configuration is complete, view the global routing table on the device.

Take PE1 as an example:

```
PE1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

O 11.11.11.11/32 [110/2] via 93.1.1.1, 03:19:45, vlan2
C 93.1.0.0/16 is directly connected, 03:20:31, vlan2
L 93.1.1.2/32 is directly connected, 03:20:31, vlan2
LC 90.90.90.90/32 is directly connected, 03:22:09, loopback0
```

It is indicated that the global routing table of PE1 has the routing information of the loopback port of PE2 present.

---

 **Note**

- Refer to PE1 for the inspection method of PE2.
- 

Step 4: Enable MPLS IP and MPLS LDP.

#Enable global MPLS IP and MPLS LDP on PE1, and also enable MPLS IP and MPLS LDP on the interface.

```
PE1(config)#mpls ip
PE1(config)#mpls ldp
PE1(config-ldp)#router-id 90.90.90.90
PE1(config-ldp)#address-family ipv4
PE1(config-ldp-af4)#transport-address 90.90.90.90
PE1(config-ldp-af4)#exit
PE1(config-ldp)#exit
PE1(config)#interface vlan2
PE1(config-if-vlan2)#mpls ip
PE1(config-if-vlan2)#mpls ldp
```

```
PE1(config-if-vlan2)#exit
```

# Enable global MPLS IP and MPLS LDP on PE2, and also enable MPLS IP and MPLS LDP on the interface.

```
PE2(config)#mpls ip
PE2(config)#mpls ldp
PE2(config-ldp)#router-id 11.11.11.11
PE2(config-ldp)#address-family ipv4
PE2(config-ldp-af4)#transport-address 11.11.11.11
PE2(config-ldp-af4)#exit
PE2(config-ldp)#exit
PE2(config)#interface vlan2
PE2(config-if-vlan2)#mpls ip
PE2(config-if-vlan2)#mpls ldp
PE2(config-if-vlan2)#exit
```

# After the configuration is complete, view the LDP session information on the device.

Take PE1 as an example:

```
PE1#show mpls ldp session
Peer IP Address  Peer Type  My Role  State    DS Cap  DeadTime
11.11.11.11     Multicast  Active   OPERATIONAL  Disabled 00:02:19
Statistics for ldp sessions:
  Multicast sessions: 1
  Targeted sessions: 0
```

It is indicated that PE1 and PE2 successfully establish the LDP session.

#View the routing label table entries on the device.

Take PE1 as an example:

```
PE1#show ip route 11.11.11.11 detail
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

O 11.11.11.11/32 [110/2] via 93.1.1.1, label 3, 03:29:21, vlan2
   93.1.1.1 [0], vlan2
```

It is indicated that the label information of the loopback port to PE2 exists in the route label table of PE1.

---

## Note

- Refer to PE1 for the inspection method of PE2.

Step 5: Configure the VPN instance to advertise the routes of CE1 and CE2 to PE1 via OSPF.

#Configure VPN instance on PE1 and configure EBGP under VPN1 and RIP under VPN2.

```
PE1(config)#ip vrf 1
PE1(config-vrf)#rd 100:1
PE1(config-vrf)#route-target export 100:1
PE1(config-vrf)#route-target import 100:1
PE1(config-vrf)#exit
PE1(config)#ip vrf 2
PE1(config-vrf)#rd 200:1
PE1(config-vrf)#route-target export 200:1
PE1(config-vrf)#route-target import 200:1
PE1(config-vrf)#exit
PE1(config)#interface vlan3
PE1(config-if-vlan3)#ip vrf forwarding 1
PE1(config-if-vlan3)#ip address 95.1.1.1 255.255.0.0
PE1(config-if-vlan3)#exit
PE1(config)#interface vlan4
PE1(config-if-vlan4)#ip vrf forwarding 2
PE1(config-if-vlan4)#ip address 94.1.1.1 255.255.0.0
PE1(config-if-vlan4)#exit
PE1(config)#router bgp 100
PE1(config-bgp)#address-family ipv4 vrf 1
PE1(config-bgp-af)#neighbor 95.1.1.2 remote-as 200
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
PE1(config)#router rip
PE1(config-rip)#address-family ipv4 vrf 2
PE1(config-rip-af)#version 2
PE1(config-rip-af)#network 94.1.0.0
PE1(config-rip-af)#exit-address-family
PE1(config-rip)#exit
```

#Configure EBGP on CE1 to advertise CE routes to the PE.

```
CE1#configure terminal
CE1(config)#router bgp 200
CE1(config-bgp)#neighbor 95.1.1.1 remote-as 100
CE1(config-bgp)#network 5.5.5.5 255.255.255.255
CE1(config-bgp)#network 95.1.0.0 255.255.0.0
```

```
CE1(config-bgp)#exit
```

#Configure RIP on CE2 to advertise CE routes to the PE.

```
CE2#configure terminal
CE2(config)#router rip
CE2(config-rip)#version 2
CE2(config-rip)#network 2.2.2.2
CE2(config-rip)#network 94.1.0.0
CE2(config-rip)#exit
```

#After the configuration is complete, check the routing table of VPN1 and VPN2 on PE1.

```
PE1#show ip route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
B 5.5.5.5/32 [20/0] via 95.1.1.2, 03:22:26, vlan3
C 95.1.0.0/16 is directly connected, 03:48:37, vlan3
L 95.1.1.1/32 is directly connected, 03:48:37, vlan3
```

```
PE1#show ip route vrf 2
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
R 2.2.2.2/32 [120/1] via 94.1.1.2, 03:46:36, vlan4
C 94.1.0.0/16 is directly connected, 03:58:11, vlan4
L 94.1.1.1/32 is directly connected, 03:58:11, vlan4
```

It is indicated that routes to CE1 and CE2 exist in the VPN1 and VPN2 routing tables of PE1.

Step 6: Configure VPN instances on PE2 and MCE, and configure default routes on CE3 and CE4 to point to MCE.

#Configure VPN instance on PE2 and configure OSPF under VPN1 and VPN2.

```
PE2(config)#ip vrf 1
PE2(config-vrf)#rd 100:1
PE2(config-vrf)#route-target export 100:1
```

```

PE2(config-vrf)#route-target import 100:1
PE2(config-vrf)#exit
PE2(config)#ip vrf 2
PE2(config-vrf)#rd 200:1
PE2(config-vrf)#route-target export 200:1
PE2(config-vrf)#route-target import 200:1
PE2(config-vrf)#exit
PE2(config)#interface vlan4
PE2(config-if-vlan4)#ip vrf forwarding 1
PE2(config-if-vlan4)#ip address 92.1.1.1 255.255.0.0
PE2(config-if-vlan4)#exit
PE2(config)#interface vlan3
PE2(config-if-vlan3)#ip vrf forwarding 2
PE2(config-if-vlan3)#ip address 97.1.1.2 255.255.0.0
PE2(config-if-vlan3)#exit
PE2(config)#router ospf 200 vrf 1
PE2(config-ospf)#network 92.1.0.0 0.0.255.255 area 0
PE2(config-ospf)#exit
PE2(config)#router ospf 300 vrf 2
PE2(config-ospf)#network 97.1.0.0 0.0.255.255 area 0
PE2(config-ospf)#exit

```

**#Configure VPN instance on MCE and configure OSPF under VPN1 and VPN2, configure static route to CE loopback port and redistribute it into OSPF.**

```

MCE#configure terminal
MCE(config)#ip vrf 1
MCE(config-vrf)#rd 100:1
MCE(config-vrf)#exit
MCE(config)#ip vrf 2
MCE(config-vrf)#rd 200:1
MCE(config-vrf)#exit
MCE(config)#interface vlan4
MCE(config-if-vlan4)#ip vrf forwarding 1
MCE(config-if-vlan4)#ip address 92.1.1.2 255.255.0.0
MCE(config-if-vlan4)#exit
MCE(config)#interface vlan3
MCE(config-if-vlan3)#ip vrf forwarding 2
MCE(config-if-vlan3)#ip address 97.1.1.1 255.255.0.0
MCE(config-if-vlan3)#exit
MCE(config)#interface vlan2
MCE(config-if-vlan2)#ip vrf forwarding 1

```

```
MCE(config-if-vlan2)#ip address 90.1.1.1 255.255.0.0
MCE(config-if-vlan2)#exit
MCE(config)#interface vlan5
MCE(config-if-vlan5)#ip vrf forwarding 2
MCE(config-if-vlan5)#ip address 91.1.1.1 255.255.0.0
MCE(config-if-vlan5)#exit
MCE(config)#ip route vrf 1 8.8.8.8 255.255.255.255 90.1.1.2
MCE(config)#ip route vrf 2 3.3.3.3 255.255.255.255 91.1.1.2
MCE(config)#router ospf 100 vrf 1
MCE(config-ospf)#network 90.1.0.0 0.0.255.255 area 0
MCE(config-ospf)#network 92.1.0.0 0.0.255.255 area 0
MCE(config-ospf)#redistribute static
MCE(config-ospf)#exit
MCE(config)#router ospf 200 vrf 2
MCE(config-ospf)#network 91.1.0.0 0.0.255.255 area 0
MCE(config-ospf)#network 97.1.0.0 0.0.255.255 area 0
MCE(config-ospf)#redistribute static
MCE(config-ospf)#exit
```

#Configure the default route on CE3 with the outgoing interface pointing to the MCE.

```
CE3#configure terminal
CE3(config)#ip route 0.0.0.0 0.0.0.0 90.1.1.1
```

#Configure the default route on CE4 with the outgoing interface pointing to the MCE.

```
CE4#configure terminal
CE4(config)#ip route 0.0.0.0 0.0.0.0 91.1.1.1
```

---

## Note

- Only one default route needs to be configured on CE3 and CE4, with the outgoing interface pointing to the MCE.
- 

#After the configuration is complete, view the routing table of VPN1 and VPN2 on the MCE.

```
MCE#show ip route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
S 8.8.8.8/32 [1/10] via 90.1.1.2, 20:18:48, vlan2
C 90.1.0.0/16 is directly connected, 22:59:50, vlan2
L 90.1.1.1/32 is directly connected, 22:59:50, vlan2
C 92.1.0.0/16 is directly connected, 01:02:01, vlan4
L 92.1.1.1/32 is directly connected, 01:02:01, vlan4
```

```
MCE#show ip route vrf 2
```

```
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
```

```
U - Per-user Static route
```

```
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
S 3.3.3.3/32 [1/10] via 91.1.1.2, 20:18:33, vlan5
C 91.1.0.0/16 is directly connected, 23:00:53, vlan5
L 91.1.1.1/32 is directly connected, 23:00:53, vlan5
C 97.1.0.0/16 is directly connected, 01:02:04, vlan3
L 97.1.1.2/32 is directly connected, 01:02:04, vlan3
```

It is indicated that static route information to CE3 and CE4 exists on the VPN1 and VPN2 routing tables of the MCE.

#View the routing table of VPN1 and VPN2 on PE2.

```
PE2#show ip route vrf 1
```

```
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
```

```
U - Per-user Static route
```

```
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
OE 8.8.8.8/32 [150/20] via 92.1.1.1, 00:27:44, vlan4
O 90.1.0.0/16 [110/2] via 92.1.1.1, 00:27:45, vlan4
C 92.1.0.0/16 is directly connected, 00:27:57, vlan4
L 92.1.1.2/32 is directly connected, 00:27:57, vlan4
```

```
PE2#show ip route vrf 2
```

```
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
```

```
U - Per-user Static route
```

```
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
OE 3.3.3.3/32 [150/20] via 97.1.1.2, 00:27:48, vlan3
O 91.1.0.0/16 [110/2] via 97.1.1.2, 00:27:49, vlan3
C 97.1.0.0/16 is directly connected, 00:28:00, vlan3
L 97.1.1.1/32 is directly connected, 00:28:00, vlan3
```

It is indicated that the routing information to CE3 and CE4 exists on the VPN1 and VPN2 routing tables of PE2.

**Step 7:** Configure the MP-IBGP to use the loopback interface as the peer address; and redistribute routes with each other and the IGP protocol under the VPN instance.

#Configure the MP-IBGP on PE1 to enable VPNv4 address clustering; and redistribute routes with each other and the IGP protocol under the VPN instance.

```
PE1(config)#router bgp 100
PE1(config-bgp)#neighbor 11.11.11.11 remote-as 100
PE1(config-bgp)#neighbor 11.11.11.11 update-source loopback0
PE1(config-bgp)#address-family vpnv4
PE1(config-bgp-af)#neighbor 11.11.11.11 activate
PE1(config-bgp-af)#neighbor 11.11.11.11 send-community extended
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#address-family ipv4 vrf 2
PE1(config-bgp-af)#redistribute rip
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
PE1(config)#router rip
PE1(config-rip)#address-family ipv4 vrf 2
PE1(config-rip-af)#redistribute bgp 100
PE1(config-rip-af)#exit-address-family
PE1(config-rip)#exit
```

#Configure the MP-IBGP on PE2 to enable VPNv4 address clustering; and redistribute routes with each other and the IGP protocol under the VPN instance.

```
PE2(config)#router bgp 100
PE2(config-bgp)#neighbor 90.90.90.90 remote-as 100
PE2(config-bgp)#neighbor 90.90.90.90 update-source loopback0
PE2(config-bgp)#address-family vpnv4
PE2(config-bgp-af)#neighbor 90.90.90.90 activate
PE2(config-bgp-af)#neighbor 90.90.90.90 send-community extended
PE2(config-bgp-af)#exit-address-family
```

```

PE2(config-bgp)#address-family ipv4 vrf 1
PE2(config-bgp-af)#redistribute ospf 200
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#address-family ipv4 vrf 2
PE2(config-bgp-af)#redistribute ospf 300
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#exit
PE2(config)#router ospf 200 vrf 1
PE2(config-ospf)#redistribute bgp 100
PE2(config-ospf)#exit
PE2(config)#router ospf 300 vrf 2
PE2(config-ospf)#redistribute bgp 100
PE2(config-ospf)#exit

```

Step 8: Check the result.

# After the configuration is complete, view the BGP neighbor information on the PE.

Take PE1 as an example:

```

PE1#show ip bgp vpnv4 all summary
BGP router identifier 90.90.90.90, local AS number 100
BGP table version is 4
2 BGP AS-PATH entries
0 BGP community entries

Neighbor    V  AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State/PfxRcd
11.11.11.11 4  100   11    12    4    0  00:07:25    6

Total number of neighbors 1
BGP VRF 1 Route Distinguisher:
100:1
BGP table version is 1
2 BGP AS-PATH entries
0 BGP community entries

Neighbor    V  AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State/PfxRcd
95.1.1.2    4  200    8    7    1    0  00:04:20    2

Total number of neighbors 1

```

The successful establishment of BGP neighbors by PE1 with PE2 and CE1 can be seen from the fact that the contents of the column State/PfxRcd are shown as numbers (the number of received route prefixes from neighbors).

#View the BGP VPNv4 routing table and VPN routing table on the PE.

Take PE1 as an example:

```

PE1#show ip bgp vpnv4 vrf 1

BGP table version is 33, local router ID is 90.90.90.90

Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
                S Stale

Origin codes: i - IGP, e - EGP, ? - incomplete

```

Network	Next Hop	Metric	LocPrf	Weight	Path
Route Distinguisher: 100:1 (Default for VRF 1)					
[B]*> 5.5.5.5/32	95.1.1.2	0	0	200	i
[B]*>i8.8.8.8/32	11.11.11.11	20	100	0	?
[B]*>i90.1.0.0/16	11.11.11.11	2	100	0	?
[B]*>i92.1.0.0/16	11.11.11.11	1	100	0	?
[B]*> 95.1.0.0/16	95.1.1.2	0	0	200	i

PE1#show ip bgp vpnv4 vrf 2

BGP table version is 33, local router ID is 90.90.90.90

Status codes: s suppressed, d damped, h history, \* valid, > best, i - internal,

S Stale

Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
Route Distinguisher: 200:1 (Default for VRF 2)					
[R]*> 2.2.2.2/32	94.1.1.2	1	32768	?	
[B]*>i3.3.3.3/32	11.11.11.11	20	100	0	?
[B]*>i91.1.0.0/16	11.11.11.11	2	100	0	?
[R]*> 94.1.0.0/16	0.0.0.0	1	32768	?	
[B]*>i97.1.0.0/16	11.11.11.11	1	100	0	?

PE1#show ip route vrf 1

Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS

U - Per-user Static route

O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

B 5.5.5.5/32 [20/0] via 95.1.1.2, 22:47:14, vlan3  
 B 8.8.8.8/32 [200/20] via 11.11.11.11, 00:07:03, vlan2  
 B 90.1.0.0/16 [200/2] via 11.11.11.11, 00:07:03, vlan2  
 B 92.1.0.0/16 [200/1] via 11.11.11.11, 00:07:03, vlan2  
 C 95.1.0.0/16 is directly connected, 23:13:25, vlan3  
 L 95.1.1.1/32 is directly connected, 23:13:25, vlan3

PE1#show ip route vrf 2

Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS

U - Per-user Static route

O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

```

R 2.2.2/32 [120/1] via 94.1.1.2, 22:59:23, vlan4
B 3.3.3/32 [200/20] via 11.11.11.11, 00:07:05, vlan2
B 91.1.0.0/16 [200/2] via 11.11.11.11, 00:07:05, vlan2
C 94.1.0.0/16 is directly connected, 23:10:58, vlan4
L 94.1.1.1/32 is directly connected, 23:10:58, vlan4
B 97.1.0.0/16 [200/1] via 11.11.11.11, 00:07:05, vlan2

```

It is indicated the route information to the peer CE3 and CE4 under the BGP VPNv4 routing table, VPN1 and VPN2 routing table of PE1.

#View the routing label information on the PE.

Take PE1 as an example:

```

PE1#show ip route vrf 1 8.8.8.8 detail
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
        U - Per-user Static route
        O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

```

```

B 8.8.8/32 [200/0] via 11.11.11.11, label 16, 01:04:26, vlan2
    93.1.1.1 [2], label 3, vlan2

```

```

PE1#show ip route vrf 2 3.3.3.3 detail
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
        U - Per-user Static route
        O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

```

```

B 3.3.3/32 [200/0] via 11.11.11.11, label 17, 01:04:26, vlan2
    93.1.1.1 [2], label 3, vlan2

```

```

PE1#show mpls forwarding-table
Pro: L - LDP, B - MP-BGP, R - RSVP, M - Mapped-Route, ML - mLDP (ML FEC: Root
address/OT/OV), RM - RSVP P2MP (RM FEC: P2MP ID/TID)
        S - Static Label

```

Pro	Ident	FEC	Inlabel	Outlabel	Outgoing	Next hop
B	1	0.0.0.0/0	5120	/	/	/

It is indicated that the route label information of VPN1 and VPN2 exists in the MPLS forwarding table of PE1.

---

 **Note**

- Refer to PE1 for the inspection method of PE2.
- 

#Ping the loopback port of CE3 on CE1 to see if it can ping through.

```
CE1#ping 8.8.8.8
```

```
Press key (ctrl + shift + 6) interrupt it.
```

```
Sending 5, 76-byte ICMP Echos to 8.8.8.8 , timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100% (5/5). Round-trip min/avg/max = 0/0/0 ms.
```

#Ping the loopback port of CE4 on CE1 to see if it can ping through.

```
CE1#ping 3.3.3.3
```

```
Press key (ctrl + shift + 6) interrupt it.
```

```
Sending 5, 76-byte ICMP Echos to 3.3.3.3 , timeout is 2 seconds:
```

```
.....
```

```
Success rate is 0% (0/5).
```

It is indicated that devices within the same VPN can communicate normally, while devices in different VPNs cannot communicate and routes are isolated.

### 79.3.3 Configure Cross-domain Option-A

#### Network Requirements

- The entire MPLS network includes two AS domains, and CE1 in AS 100 needs to communicate with CE2 in AS 200.
- CE1 and CE2 belong to VPN1 at the same time and use OSPF to connect to the PE.
- The ASBRs use the VRF-to-VRF method to interact with each other for VPN routes.

- The Route-Target of VPN instances of different ASes need not match.
- The ASBR uses MP-IBGP for routing interactions with the PE.

### Network Topology

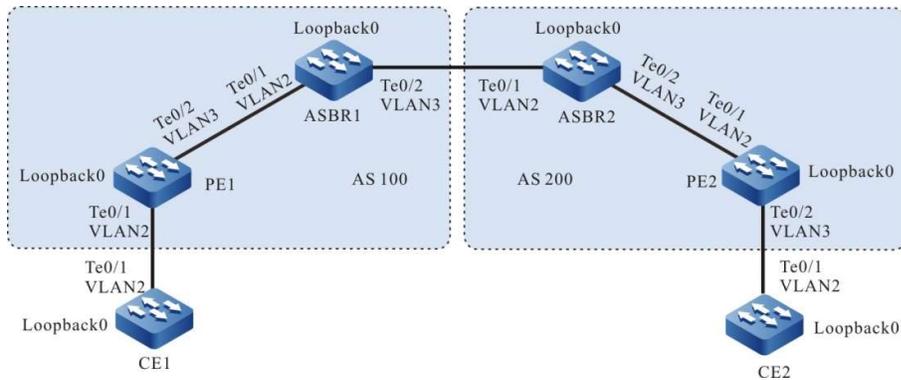


Figure 79-14 Network Topology for Configuring Cross-Domain OptionA

Table 39-40 Interface Mapping Relationships

of equipment	Interface	IP address	of equipment	Interface	IP address
CE1	Vlan2	10.1.1.1/24	ASBR2	Vlan2	10.1.3.2/24
	Loopback0	1.1.1.1/32		Vlan3	10.1.4.1/24
PE1	Vlan2	10.1.1.2/24		Loopback0	33.33.33.33/32
	Vlan3	10.1.2.1/24	PE2	Vlan2	10.1.4.2/24
	Loopback0	11.11.11.11/32		Vlan3	10.1.5.1/24
ASBR1	Vlan2	10.1.2.2/24		Loopback0	44.44.44.44/32
	Vlan3	10.1.3.1/24	CE2	Vlan2	10.1.5.2/24
	Loopback0	22.22.22.22/32		Loopback0	2.2.2.2/32

### Configuration Steps

- Step 1: Configure the VLAN and add the port to the corresponding VLAN in access mode. (Omitted)
- Step 2: Configure IP addresses for the ports. (Omitted)
- Step 3: Configure a global OSPF to advertise global route within the same AS domain.

#Configure global OSPF on PE1.

```
PE1#configure terminal
PE1(config)#router ospf 100
PE1(config-ospf)#network 10.1.2.0 0.0.0.255 area 0
PE1(config-ospf)#network 11.11.11.11 0.0.0.0 area 0
PE1(config-ospf)#exit
```

# Configure global OSPF on ASBR1.

```
ASBR1#configure terminal
ASBR1(config)#router ospf 100
ASBR1(config-ospf)#network 10.1.2.0 0.0.0.255 area 0
ASBR1(config-ospf)#network 22.22.22.22 0.0.0.0 area 0
ASBR1(config-ospf)#exit
```

# Configure global OSPF on ASBR2.

```
ASBR2#configure terminal
ASBR2(config)#router ospf 100
ASBR2(config-ospf)#network 10.1.4.0 0.0.0.255 area 0
ASBR2(config-ospf)#network 33.33.33.33 0.0.0.0 area 0
ASBR2(config-ospf)#exit
```

#Configure global OSPF on PE2.

```
PE2#configure terminal
PE2(config)#router ospf 100
PE2(config-ospf)#network 10.1.4.0 0.0.0.255 area 0
PE2(config-ospf)#network 44.44.44.44 0.0.0.0 area 0
PE2(config-ospf)#exit
```

#After the configuration is complete, view the global routing table on the device.

Take PE1 as an example:

```
PE1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
C 10.1.2.0/24 is directly connected, 69:53:53, vlan3
L 10.1.2.1/32 is directly connected, 69:53:53, vlan3
LC 11.11.11.11/32 is directly connected, 69:53:37, loopback0
O 22.22.22.22/32 [110/2] via 10.1.2.2, 48:14:20, vlan3
C 127.0.0.0/8 is directly connected, 1183:09:57, lo0
```

It is indicated that the route information of ASBR1 loopback port exists in the global routing table of PE1.

---

## Note

- Refer to PE1 for the inspection method of PE2 and ASBR.
- 

Step 4: Enable MPLS IP and MPLS LDP.

#Enable global MPLS IP and MPLS LDP on PE1, and also enable MPLS IP and MPLS LDP on the interface.

```
PE1(config)#mpls ip
PE1(config)#mpls ldp
PE1(config-ldp)#router-id 11.11.11.11
PE1(config-ldp)#address-family ipv4
PE1(config-ldp-af4)#transport-address 11.11.11.11
PE1(config-ldp-af4)#exit
PE1(config-ldp)#exit
PE1(config)#interface vlan3
PE1(config-if-vlan3)#mpls ldp
PE1(config-if-vlan3)#mpls ip
PE1(config-if-vlan3)#exit
```

# Enable global MPLS IP and MPLS LDP on ASBR1, and also enable MPLS IP and MPLS LDP on the interface.

```
ASBR1(config)#mpls ip
ASBR1(config)#mpls ldp
ASBR1(config-ldp)#router-id 22.22.22.22
ASBR1(config-ldp)#address-family ipv4
ASBR1(config-ldp-af4)#transport-address 22.22.22.22
ASBR1(config-ldp-af4)#exit
ASBR1(config-ldp)#exit
ASBR1(config)#interface vlan2
ASBR1(config-if-vlan2)#mpls ip
ASBR1(config-if-vlan2)#mpls ldp
ASBR1(config-if-vlan2)#exit
```

# Enable global MPLS IP and MPLS LDP on ASBR2, and also enable MPLS IP and MPLS LDP on the interface.

```
ASBR2(config)#mpls ip
ASBR2(config)#mpls ldp
```

```

ASBR2(config-ldp)#router-id 33.33.33.33
ASBR2(config-ldp)#address-family ipv4
ASBR2(config-ldp-af4)#transport-address 33.33.33.33
ASBR2(config-ldp-af4)#exit
ASBR2(config-ldp)#exit
ASBR2(config)#interface vlan3
ASBR2(config-if-vlan3)#mpls ldp
ASBR2(config-if-vlan3)#mpls ip
ASBR2(config-if-vlan3)#exit

```

# Enable global MPLS IP and MPLS LDP on PE2, and also enable MPLS IP and MPLS LDP on the interface.

```

PE2(config)#mpls ip
PE2(config)#mpls ldp
PE2(config-ldp)#router-id 44.44.44.44
PE2(config-ldp)#address-family ipv4
PE2(config-ldp-af4)#transport-address 44.44.44.44
PE2(config-ldp-af4)#exit
PE2(config-ldp)#exit
PE2(config)#interface vlan2
PE2(config-if-vlan2)#mpls ip
PE2(config-if-vlan2)#mpls ldp
PE2(config-if-vlan2)#exit

```

# After the configuration is complete, view the LDP session information on the device.

Take PE1 as an example:

```

PE1#show mpls ldp session
Peer IP Address  Peer Type  My Role  State    DS Cap  DeadTime
22.22.22.22     Multicast  Passive  OPERATIONAL  Disabled 00:02:34
Statistics for ldp sessions:
  Multicast sessions: 1
  Targeted sessions: 0

```

It is indicated that PE1 has established LDP session with ASBR1 successfully.

#View the routing label table entries on the device.

Take PE1 as an example:

```

PE1#show ip route 22.22.22.22 detail
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

```

O 22.22.22.22/32 [110/2] via 10.1.2.2, label 3, 14:29:21, vlan3  
10.1.2.2 [0], vlan3

It is indicated that the routing table of PE1 has the label information to the ASBR1 loopback port.

---

## Note

- Refer to PE1 for the inspection method of PE2 and ASBR.
- 

Step 5: Configure the VPN instance to advertise the CE route to the PE via OSPF.

#Configure OSPF on CE1.

```
CE1#configure terminal
CE1(config)#router ospf 100
CE1(config-ospf)#network 1.1.1.1 0.0.0.0 area 0
CE1(config-ospf)#network 10.1.1.0 0.0.0.255 area 0
CE1(config-ospf)#exit
```

#Configure VPN instance and OSPF under VPN on PE1.

```
PE1(config)#ip vrf 1
PE1(config-vrf)#rd 100:1
PE1(config-vrf)#route-target export 100:1
PE1(config-vrf)#route-target import 100:1
PE1(config-vrf)#exit
PE1(config)#interface vlan2
PE1(config-if-vlan2)#ip vrf forwarding 1
PE1(config-if-vlan2)#ip address 10.1.1.2 255.255.255.0
PE1(config-if-vlan2)#exit
PE1(config)#router ospf 200 vrf 1
PE1(config-ospf)#network 10.1.1.0 0.0.0.255 area 0
PE1(config-ospf)#exit
```

#Configure VPN instance on ASBR1.

```
ASBR1(config)#ip vrf 1
ASBR1(config-vrf)#rd 100:1
ASBR1(config-vrf)#route-target export 100:1
ASBR1(config-vrf)#route-target import 100:1
ASBR1(config-vrf)#exit
```

```
ASBR1(config)#interface vlan3
ASBR1(config-if-vlan3)#ip vrf forwarding 1
ASBR1(config-if-vlan3)#ip address 10.1.3.1 255.255.255.0
ASBR1(config-if-vlan3)#exit
```

#Configure VPN instance on ASBR2.

```
ASBR2(config)#ip vrf 1
ASBR2(config-vrf)#rd 200:1
ASBR2(config-vrf)#route-target export 200:1
ASBR2(config-vrf)#route-target import 200:1
ASBR2(config-vrf)#exit
ASBR2(config)#interface vlan2
ASBR2(config-if-vlan2)#ip vrf forwarding 1
ASBR2(config-if-vlan2)#ip address 10.1.3.2 255.255.255.0
ASBR2(config-if-vlan2)#exit
```

#Configure VPN instance and OSPF under VPN on PE2.

```
PE2(config)#ip vrf 1
PE2(config-vrf)#rd 200:1
PE2(config-vrf)#route-target export 200:1
PE2(config-vrf)#route-target import 200:1
PE2(config-vrf)#exit
PE2(config)#interface vlan3
PE2(config-if-vlan3)#ip vrf forwarding 1
PE2(config-if-vlan3)#ip address 10.1.5.1 255.255.255.0
PE2(config-if-vlan3)#exit
PE2(config)#router ospf 200 vrf 1
PE2(config-ospf)#network 10.1.5.0 0.0.0.255 area 0
PE2(config-ospf)#exit
```

#Configure OSPF on CE2.

```
CE2#configure terminal
CE2(config)#router ospf 100
CE2(config-ospf)#network 2.2.2.2 0.0.0.0 area 0
CE2(config-ospf)#network 10.1.5.0 0.0.0.255 area 0
CE2(config-ospf)#exit
```

#After the configuration is complete, view the VPN routing table on the PE.

Take PE1 as an example:

```
PE1#show ip route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
```

```
O 1.1.1.1/32 [110/2] via 10.1.1.1, 70:07:57, vlan2
C 10.1.1.0/24 is directly connected, 70:09:30, vlan2
L 10.1.1.2/32 is directly connected, 70:09:30, vlan2
```

It is indicated that a route to CE1 exists in the VPN1 routing table of PE1.

---

## Note

- Refer to PE1 for the inspection method of PE2.
- 

Step 6: Configure the MP-IBGP between the PE and the ASBR, using the loopback interface as the peer address; configure EBGP between the ASBR and redistribute routes with each other and the IGP protocol under the VPN instance.

#Configure the MP-IBGP on PE1 to enable VPNv4 address clustering; and redistribute routes with each other and the IGP protocol under the VPN instance.

```
PE1(config)#router bgp 100
PE1(config-bgp)#neighbor 22.22.22.22 remote-as 100
PE1(config-bgp)#neighbor 22.22.22.22 update-source loopback0
PE1(config-bgp)#address-family vpnv4
PE1(config-bgp-af)#neighbor 22.22.22.22 activate
PE1(config-bgp-af)#neighbor 22.22.22.22 send-community extended
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#address-family ipv4 vrf 1
PE1(config-bgp-af)#redistribute ospf 200
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
PE1(config)#router ospf 200
PE1(config-ospf)#redistribute bgp 100
PE1(config-ospf)#exit
```

#Configure the MP-IBGP between ASBR1 and PE1 with VPNv4 address clusters enabled; and configure EBGP between ASBR2 under VRF address clusters.

```
ASBR1(config)#router bgp 100
```

```
ASBR1(config-bgp)#neighbor 11.11.11.11 remote-as 100
ASBR1(config-bgp)#neighbor 11.11.11.11 update-source loopback0
ASBR1(config-bgp)#address-family vpv4
ASBR1(config-bgp-af)#neighbor 11.11.11.11 activate
ASBR1(config-bgp-af)#neighbor 11.11.11.11 send-community extended
ASBR1(config-bgp-af)#exit-address-family
ASBR1(config-bgp)#address-family ipv4 vrf 1
ASBR1(config-bgp-af)#redistribute connected
ASBR1(config-bgp-af)#neighbor 10.1.3.2 remote-as 200
ASBR1(config-bgp-af)#exit-address-family
ASBR1(config-bgp)#exit
```

#Configure the MP-IBGP between ASBR2 and PE2 with VPNv4 address clusters enabled; and configure EBGP between ASBR1 under VRF address clusters.

```
ASBR2(config)#router bgp 200
ASBR2(config-bgp)#neighbor 44.44.44.44 remote-as 200
ASBR2(config-bgp)#neighbor 44.44.44.44 update-source loopback0
ASBR2(config-bgp)#address-family vpv4
ASBR2(config-bgp-af)#neighbor 44.44.44.44 activate
ASBR2(config-bgp-af)#neighbor 44.44.44.44 send-community extended
ASBR2(config-bgp-af)#exit-address-family
ASBR2(config-bgp)#address-family ipv4 vrf 1
ASBR2(config-bgp-af)#redistribute connected
ASBR2(config-bgp-af)#neighbor 10.1.3.1 remote-as 100
ASBR2(config-bgp-af)#exit-address-family
ASBR2(config-bgp)#exit
```

#Configure the MP-IBGP on PE2 to enable VPNv4 address clustering; and redistribute routes with each other and the IGP protocol under the VPN instance.

```
PE2(config)#router bgp 200
PE2(config-bgp)#neighbor 33.33.33.33 remote-as 200
PE2(config-bgp)#neighbor 33.33.33.33 update-source loopback0
PE2(config-bgp)#address-family vpv4
PE2(config-bgp-af)#neighbor 33.33.33.33 activate
PE2(config-bgp-af)#neighbor 33.33.33.33 send-community extended
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#address-family ipv4 vrf 1
PE2(config-bgp-af)#redistribute ospf 200
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#exit
PE2(config)#router ospf 200 vrf 1
PE2(config-ospf)#redistribute bgp 200
```

```
PE2(config-ospf)#exit
```

Step 7: Check the result.

# After the configuration is completed, check the BGP neighbor information on the PE and ASBR.

Take PE1, ASBR1 as an example.

```
PE1#show ip bgp vpnv4 all summary
```

```
BGP router identifier 11.11.11.11, local AS number 100
```

```
BGP table version is 6
```

```
1 BGP AS-PATH entries
```

```
0 BGP community entries
```

```
Neighbor    V  AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down State/PfxRcd
22.22.22.22 4 100   44   43    6   0  00:34:07   3
```

```
Total number of neighbors 1
```

The successful establishment of BGP neighbors between PE1 and ASBR1 can be seen from the fact that the contents of the column State/PfxRcd are shown as numbers (the number of received route prefixes from neighbors).

```
ASBR1#show ip bgp vpnv4 all summary
```

```
BGP router identifier 22.22.22.22, local AS number 100
```

```
BGP table version is 5
```

```
2 BGP AS-PATH entries
```

```
0 BGP community entries
```

```
Neighbor    V  AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down State/PfxRcd
11.11.11.11 4 100   20   21    4   0  00:14:56   2
```

```
Total number of neighbors 1
```

```
BGP VRF 1 Route Distinguisher:
```

```
100:1
```

```
BGP table version is 1
```

```
2 BGP AS-PATH entries
```

```
0 BGP community entries
```

```
Neighbor    V  AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down State/PfxRcd
10.1.3.2    4 200    3    3    1   0  00:00:03   3
```

```
Total number of neighbors 1
```

The successful establishment of BGP neighbors between ASBR1 and PE1 and ASBR2 can be seen from the fact that the contents of this column of State/PfxRcd are shown as numbers (the number of received route prefixes from neighbors).

#View the BGP VPNv4 routing table on the PE and ASBR.

Take PE1, ASBR1 as an example.

```
PE1#show ip bgp vpnv4 vrf 1
BGP table version is 28, local router ID is 11.11.11.11
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop        Metric LocPrf Weight Path
Route Distinguisher: 100:1 (Default for VRF 1)
[O]*> 1.1.1.1/32   10.1.1.1         2    32768 ?
[B]*>i2.2.2.2/32   22.22.22.22      0  100  0 200 ?
[O]*> 10.1.1.0/24  0.0.0.0          1    32768 ?
[B]*>i10.1.3.0/24  22.22.22.22      0  100  0 ?
[B]*>i10.1.5.0/24  22.22.22.22      0  100  0 200 ?
```

```
ASBR1#show ip bgp vpnv4 vrf 1
BGP table version is 386, local router ID is 22.22.22.22
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop        Metric LocPrf Weight Path
Route Distinguisher: 100:1 (Default for VRF 1)
[B]*>i1.1.1.1/32   11.11.11.11      2  100  0 ?
[B]*> 2.2.2.2/32   10.1.3.2          0    0 200 ?
[B]*>i10.1.1.0/24  11.11.11.11      1  100  0 ?
[B]* 10.1.3.0/24   10.1.3.2          0    0 200 ?
[C]*>              0.0.0.0           0    32768 ?
[B]*> 10.1.5.0/24  10.1.3.2          0    0 200 ?
```

It is indicated the BGP routing information to the peer CE2 exists in the BGP VPNv4 routing table of PE1 and ASBR1.

#View the route label table entries and MPLS forwarding table entries on the PE and ASBR.

Take PE1, ASBR1 as an example.

```
PE1#show ip route vrf 1 1.1.1.1 detail
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
```

O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

O 1.1.1.1/32 [110/2] via 10.1.1.1, 01:05:26, vlan2  
10.1.1.1 [0], vlan2

PE1#show ip route vrf 1 2.2.2.2 detail

Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS

U - Per-user Static route

O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

B 2.2.2.2/32 [200/0] via 22.22.22.22, label 20480, 01:04:26, vlan3  
10.1.2.2 [2], label 3, vlan3

PE1#show mpls forwarding-table

Pro: L - LDP, B - MP-BGP, R - RSVP, M - Mapped-Route, ML - mLDP (ML FEC: Root address/OT/OV), RM - RSVP P2MP (RM FEC: P2MP ID/TID)

S - Static Label

Pro	Ident	FEC	Inlabel	Outlabel	Outgoing	Next hop
B	1	0.0.0.0/0	5120	/	/	/

ASBR1#show ip route vrf 1 1.1.1.1 detail

Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS

U - Per-user Static route

O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

B 1.1.1.1/32 [200/0] via 11.11.11.11, label 5120, 01:06:26, vlan2  
10.1.2.1 [2], label 3, vlan2

ASBR1#show ip route vrf 2.2.2.2 detail

Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS

U - Per-user Static route

O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

```
B 2.2.2.2/32 [200/0] via 10.1.3.2, 01:06:26, vlan3
    10.1.3.2 [0], vlan3
```

```
ASBR1#show mpls forwarding-table
```

```
Pro: L - LDP, B - MP-BGP, R - RSVP, M - Mapped-Route, ML - mLDP (ML FEC: Root
address/OT/OV), RM - RSVP P2MP (RM FEC: P2MP ID/TID)
```

```
S - Static Label
```

Pro Ident	FEC	Inlabel	Outlabel	Outgoing	Next hop
B 1	0.0.0.0/0	20480 /	/	/	/

It is indicated that the route label information of VPN1 exists in the route label table entries of PE1 and ASBR1.

---

## Note

- Refer to PE1 and ASBR1 for the inspection method of PE2 and ASBR2.
- 

#View the routing table on the CE.

Take CE1 as an example.

```
CE1#show ip route
```

```
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
```

```
U - Per-user Static route
```

```
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
LC 1.1.1.1/32 is directly connected, 72:03:40, loopback0
OE 2.2.2.2/32 [150/1] via 10.1.1.2, 01:12:50, vlan2
C 10.1.1.0/24 is directly connected, 72:07:55, vlan2
L 10.1.1.1/32 is directly connected, 72:07:55, vlan2
OE 10.1.3.0/24 [150/1] via 10.1.1.2, 01:14:28, vlan2
OE 10.1.5.0/24 [150/1] via 10.1.1.2, 01:12:50, vlan2
C 127.0.0.0/8 is directly connected, 210:21:32, lo0
L 127.0.0.1/32 is directly connected, 210:21:32, lo0
```

It is indicated that the routing information to the peer CE2 exists under the routing table of CE1.

#Ping the loopback port of CE2 on CE1 to see if it can ping through properly.

```
CE1#ping 2.2.2.2
```

Press key (ctrl + shift + 6) interrupt it.

Sending 5, 76-byte ICMP Echos to 2.2.2.2 , timeout is 2 seconds:

```
!!!!
```

Success rate is 100% (5/5). Round-trip min/avg/max = 0/0/0 ms.

It is indicated that CE1 can ping through to CE2.

### 79.3.4 Configure Cross-domain OptionB

#### Network Requirements

- The entire MPLS network includes two AS domains, and CE1 in AS 100 needs to communicate with CE2 in AS 200.
- CE1 and CE2 belong to VPN1 at the same time and use OSPF to interact with PEs for routing.
- The ASBRs use MP-EBGP for routing interactions between them.
- The ASBR uses MP-IBGP for routing interactions with the PE.

#### Network Topology

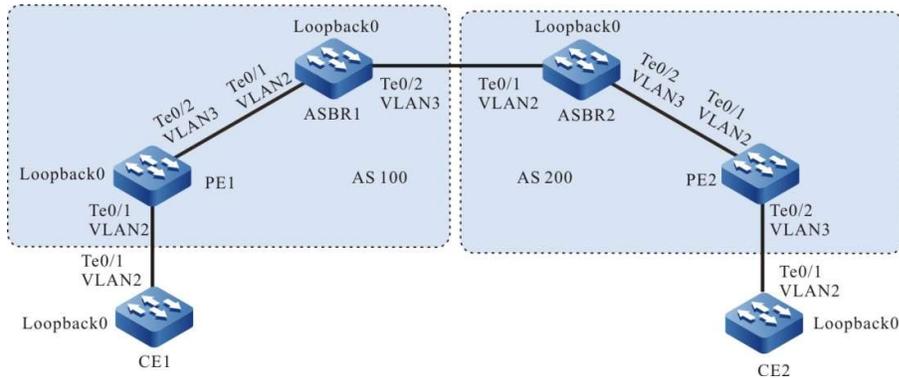


Figure 15-16 Network Topology for Configuring Cross-Domain OptionB

Table 79-41 Interface Mapping Relationships

of equipment	Interface	IP address	of equipment	Interface	IP address
CE1	Vlan2	10.1.1.1/24	ASBR2	Vlan2	10.1.3.2/24

of equipment	Interface	IP address	of equipment	Interface	IP address
	Loopback0	1.1.1.1/32		Vlan3	10.1.4.1/24
PE1	Vlan2	10.1.1.2/24		Loopback0	33.33.33.33/32
	Vlan3	10.1.2.1/24	PE2	Vlan2	10.1.4.2/24
	Loopback0	11.11.11.11/32		Vlan3	10.1.5.1/24
ASBR1	Vlan2	10.1.2.2/24		Loopback0	44.44.44.44/32
	Vlan3	10.1.3.1/24	CE2	Vlan2	10.1.5.2/24
	Loopback0	22.22.22.22/32		Loopback0	2.2.2.2/32

### Configuration Steps

Step 1: Configure the VLAN and add the port to the corresponding VLAN in access mode.  
(Omitted)

Step 2: Configure IP addresses for the ports. (Omitted)

Step 3: Configure a global OSPF to advertise global route within the same AS domain.

#Configure global OSPF on PE1.

```
PE1#configure terminal
PE1(config)#router ospf 100
PE1(config-ospf)#network 10.1.2.0 0.0.0.255 area 0
PE1(config-ospf)#network 11.11.11.11 0.0.0.0 area 0
PE1(config-ospf)#exit
```

# Configure global OSPF on ASBR1.

```
ASBR1#configure terminal
ASBR1(config)#router ospf 100
ASBR1(config-ospf)#network 10.1.2.0 0.0.0.255 area 0
ASBR1(config-ospf)#network 22.22.22.22 0.0.0.0 area 0
ASBR1(config-ospf)#exit
```

# Configure global OSPF on ASBR2.

```
ASBR2#configure terminal
ASBR2(config)#router ospf 100
ASBR2(config-ospf)#network 10.1.4.0 0.0.0.255 area 0
```

```
ASBR2(config-ospf)#network 33.33.33.33 0.0.0.0 area 0
ASBR2(config-ospf)#exit
```

#Configure global OSPF on PE2.

```
PE2#configure terminal
PE2(config)#router ospf 100
PE2(config-ospf)#network 10.1.4.0 0.0.0.255 area 0
PE2(config-ospf)#network 44.44.44.44 0.0.0.0 area 0
PE2(config-ospf)#exit
```

#After the configuration is complete, view the global routing table on the device.

Take PE1 as an example:

```
PE1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
C 10.1.2.0/24 is directly connected, 04:52:00, vlan3
L 10.1.2.1/32 is directly connected, 04:52:00, vlan3
LC 11.11.11.11/32 is directly connected, 04:51:45, loopback0
O 22.22.22.22/32 [110/2] via 10.1.2.2, 01:45:41, vlan3
C 127.0.0.0/8 is directly connected, 1118:08:05, lo0
L 127.0.0.1/32 is directly connected, 1118:08:05, lo0
```

It is indicated that the routing information of the loopback port of ASBR1 exists in the global routing table of PE1.

---

## Note

- Refer to PE1 for the inspection method of PE2 and ASBR.
- 

Step 4: Enable MPLS IP and MPLS LDP.

#Enable global MPLS IP and MPLS LDP on PE1, and also enable MPLS IP and MPLS LDP on the interface.

```
PE1(config)#mpls ip
PE1(config)#mpls ldp
```

```
PE1(config-ldp)#router-id 11.11.11.11
PE1(config-ldp)#address-family ipv4
PE1(config-ldp-af4)#transport-address 11.11.11.11
PE1(config-ldp-af4)#exit
PE1(config-ldp)#exit
PE1(config)#interface vlan3
PE1(config-if-vlan3)#mpls ldp
PE1(config-if-vlan3)#mpls ip
PE1(config-if-vlan3)#exit
```

#Enable global MPLS IP and MPLS LDP on ASBR1, and also enable MPLS IP and MPLS LDP on the interface between ASBR and PE1. The interface between ASBR only needs to enable the MPLS IP, with no need to configure the MPLS LDP.

```
ASBR1(config)#mpls ip
ASBR1(config)#mpls ldp
ASBR1(config-ldp)#router-id 22.22.22.22
ASBR1(config-ldp)#address-family ipv4
ASBR1(config-ldp-af4)#transport-address 22.22.22.22
ASBR1(config-ldp-af4)#exit
ASBR1(config-ldp)#exit
ASBR1(config)#interface vlan2
ASBR1(config-if-vlan2)#mpls ip
ASBR1(config-if-vlan2)#mpls ldp
ASBR1(config-if-vlan2)#exit
ASBR1(config)#interface vlan3
ASBR1(config-if-vlan3)#mpls ip
ASBR1(config-if-vlan3)#exit
```

#Enable global MPLS IP and MPLS LDP on ASBR2, and also enable MPLS IP and MPLS LDP on the interface between ASBR and PE2, the interface between ASBR only needs to enable MPLS IP, with no need to configure MPLS LDP.

```
ASBR2(config)#mpls ip
ASBR2(config)#mpls ldp
ASBR2(config-ldp)#router-id 33.33.33.33
ASBR2(config-ldp)#address-family ipv4
ASBR2(config-ldp-af4)#transport-address 33.33.33.33
ASBR2(config-ldp-af4)#exit
ASBR2(config-ldp)#exit
ASBR2(config)#interface vlan2
ASBR2(config-if-vlan2)#mpls ip
ASBR2(config-if-vlan2)#exit
ASBR2(config)#interface vlan3
```

```
ASBR2(config-if-vlan3)#mpls ldp
ASBR2(config-if-vlan3)#mpls ip
ASBR2(config-if-vlan3)#exit
```

# Enable global MPLS IP and MPLS LDP on PE2, and also enable MPLS IP and MPLS LDP on the interface.

```
PE2(config)#mpls ip
PE2(config)#mpls ldp
PE2(config-ldp)#router-id 44.44.44.44
PE2(config-ldp)#address-family ipv4
PE2(config-ldp-af4)#transport-address 44.44.44.44
PE2(config-ldp-af4)#exit
PE2(config-ldp)#exit
PE2(config)#interface vlan2
PE2(config-if-vlan2)#mpls ip
PE2(config-if-vlan2)#mpls ldp
PE2(config-if-vlan2)#exit
```

# After the configuration is complete, view the LDP session information on the device.

Take PE1 as an example:

```
PE1#show mpls ldp session
Peer IP Address Peer Type My Role State DS Cap DeadTime
22.22.22.22 Multicast Passive OPERATIONAL Disabled 00:02:34
Statistics for ldp sessions:
Multicast sessions: 1
Targeted sessions: 0
```

It is indicated that PE1 has established LDP session with ASBR1 successfully.

#View the routing label table entries on the device.

Take PE1 as an example:

```
PE1#show ip route 22.22.22.22 detail
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
U - Per-user Static route
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

O 22.22.22.22/32 [110/2] via 10.1.2.2, label 3, 14:29:21, vlan3
10.1.2.2 [0], vlan3
```

It is indicated that the label information to the ASBR1 loopback port exists in the route label table of PE1.

---

 **Note**

- Refer to PE1 for the inspection method of PE2 and ASBR.
- 

Step 5: Configure the VPN instance to advertise the CE route to the PE via OSPF.

#Configure VPN instance and OSPF under VPN instance on PE1.

```
PE1(config)#ip vrf 1
PE1(config-vrf)#rd 100:1
PE1(config-vrf)#route-target export 100:1
PE1(config-vrf)#route-target import 100:1
PE1(config-vrf)#exit
PE1(config)#interface vlan2
PE1(config-if-vlan2)#ip vrf forwarding 1
PE1(config-if-vlan2)#ip address 10.1.1.2 255.255.255.0
PE1(config-if-vlan2)#exit
PE1(config)#router ospf 200 vrf 1
PE1(config-ospf)#network 10.1.1.0 0.0.0.255 area 0
PE1(config-ospf)#exit
```

#Configure OSPF on CE1.

```
CE1#configure terminal
CE1(config)#router ospf 100
CE1(config-ospf)#network 1.1.1.1 0.0.0.0 area 0
CE1(config-ospf)#network 10.1.1.0 0.0.0.255 area 0
CE1(config-ospf)#exit
```

#Configure VPN instance and OSPF under VPN instance on PE2.

```
PE2(config)#ip vrf 1
PE2(config-vrf)#rd 100:1
PE2(config-vrf)#route-target export 100:1
PE2(config-vrf)#route-target import 100:1
PE2(config-vrf)#exit
PE2(config)#interface vlan3
PE2(config-if-vlan3)#ip vrf forwarding 1
PE2(config-if-vlan3)#ip address 10.1.5.1 255.255.255.0
PE2(config-if-vlan3)#exit
PE2(config)#router ospf 200 vrf 1
```

```
PE2(config-ospf)#network 10.1.5.0 0.0.0.255 area 0
PE2(config-ospf)#exit
```

#Configure OSPF on CE2.

```
CE2#configure terminal
CE2(config)#router ospf 100
CE2(config-ospf)#network 2.2.2.2 0.0.0.0 area 0
CE2(config-ospf)#network 10.1.5.0 0.0.0.255 area 0
CE2(config-ospf)#exit
```

#After the configuration is complete, view the VPN routing table on the PE.

Take PE1 as an example:

```
PE1#show ip route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

O  1.1.1.1/32 [110/2] via 10.1.1.1, 05:58:17, vlan2
C  10.1.1.0/24 is directly connected, 05:59:50, vlan2
L  10.1.1.2/32 is directly connected, 05:59:50, vlan2
```

It is indicated that a route to CE1 exists in the VPN1 routing table of PE1.

---

## Note

- Refer to PE1 for the inspection method of PE2.
- 

**Step 6:** Configure the MP-IBGP between the PE and the ASBR, using the loopback interface as the peer address; configure the MP-EBGP between the ASBR and complete route redistribution with the IGP protocol under the VPN instance.

#Configure the MP-IBGP on PE1 to enable VPNv4 address clustering; and redistribute routes with each other and the IGP protocol under the VPN instance.

```
PE1(config)#router bgp 100
PE1(config-bgp)#neighbor 22.22.22.22 remote-as 100
PE1(config-bgp)#neighbor 22.22.22.22 update-source loopback0
PE1(config-bgp)#address-family vpnv4
```

```
PE1(config-bgp-af)#neighbor 22.22.22.22 activate
PE1(config-bgp-af)#neighbor 22.22.22.22 send-community extended
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#address-family ipv4 vrf 1
PE1(config-bgp-af)#redistribute ospf 200
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
PE1(config)#router ospf 200
PE1(config-ospf)#redistribute bgp 100
PE1(config-ospf)#exit
```

#Configure the MP-IBGP on ASBR1 with PE1 and MP-EBGP between ASBR1 and ASBR2 with VPNv4 address clustering enabled.

```
ASBR1(config)#router bgp 100
ASBR1(config-bgp)#neighbor 10.1.3.2 remote-as 200
ASBR1(config-bgp)#neighbor 11.11.11.11 remote-as 100
ASBR1(config-bgp)#neighbor 11.11.11.11 update-source loopback0
ASBR1(config-bgp)#address-family vpnv4
ASBR1(config-bgp-af)#neighbor 10.1.3.2 activate
ASBR1(config-bgp-af)#neighbor 10.1.3.2 send-community extended
ASBR1(config-bgp-af)#neighbor 11.11.11.11 activate
ASBR1(config-bgp-af)#neighbor 11.11.11.11 next-hop-self
ASBR1(config-bgp-af)#neighbor 11.11.11.11 send-community extended
ASBR1(config-bgp-af)#exit-address-family
ASBR1(config-bgp)#exit
```

#Configure the MP-IBGP on ASBR2 with PE2 and MP-EBGP between ASBR2 and ASBR1 with VPNv4 address clustering enabled.

```
ASBR2(config)#router bgp 200
ASBR2(config-bgp)#neighbor 10.1.3.1 remote-as 100
ASBR2(config-bgp)#neighbor 44.44.44.44 remote-as 200
ASBR2(config-bgp)#neighbor 44.44.44.44 update-source loopback0
ASBR2(config-bgp)#address-family vpnv4
ASBR2(config-bgp-af)#neighbor 10.1.3.1 activate
ASBR2(config-bgp-af)#neighbor 10.1.3.1 send-community extended
ASBR2(config-bgp-af)#neighbor 44.44.44.44 activate
ASBR2(config-bgp-af)#neighbor 44.44.44.44 next-hop-self
ASBR2(config-bgp-af)#neighbor 44.44.44.44 send-community extended
ASBR2(config-bgp-af)#exit-address-family
ASBR2(config-bgp)#exit
```

#Configure the MP-IBGP on PE2 to enable VPNv4 address clustering; and redistribute routes with each other and the IGP protocol under the VPN instance.

```
PE2(config)#router bgp 200
PE2(config-bgp)#neighbor 33.33.33.33 remote-as 200
PE2(config-bgp)#neighbor 33.33.33.33 update-source loopback0
PE2(config-bgp)#address-family vpnv4
PE2(config-bgp-af)#neighbor 33.33.33.33 activate
PE2(config-bgp-af)#neighbor 33.33.33.33 send-community extended
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#address-family ipv4 vrf 1
PE2(config-bgp-af)#redistribute ospf 200
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#exit
PE2(config)#router ospf 200 vrf 1
PE2(config-ospf)#redistribute bgp 200
PE2(config-ospf)#exit
```

Step 7: Check the result.

# After the configuration is completed, check the BGP neighbor information on the PE and ASBR.

Take PE1, ASBR1 as an example.

```
PE1#show ip bgp vpnv4 all summary
BGP router identifier 11.11.11.11, local AS number 100
BGP table version is 1
2 BGP AS-PATH entries
0 BGP community entries

Neighbor      V  AS MsgRcvd MsgSent  TblVer  InQ  OutQ  Up/Down  State/PfxRcd
22.22.22.22   4 100    4    4    1    0  00:02:08    2

Total number of neighbors 1
```

The successful establishment of BGP neighbors between PE1 and ASBR1 can be seen from the fact that the contents of the column State/PfxRcd are shown as numbers (the number of received route prefixes from neighbors).

```
ASBR1#show ip bgp vpnv4 all summary
BGP router identifier 22.22.22.22, local AS number 100
BGP table version is 1
1 BGP AS-PATH entries
0 BGP community entries
```

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
11.11.11.11	4	100	2	2	1	0	0	00:00:14	2
10.1.3.2	4	200	7	8	1	0	0	00:05:28	2

Total number of neighbors 2

The successful establishment of BGP neighbors between ASBR1 and PE1 and ASBR2 can be seen from the fact that the contents of this column of State/PfxRcd are shown as numbers (the number of received route prefixes from neighbors).

#View the BGP VPNv4 routing table on the PE and ASBR.

Take PE1, ASBR1 as an example.

```
PE1#show ip bgp vpnv4 vrf 1
BGP table version is 8, local router ID is 11.11.11.11
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
                S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop        Metric LocPrf Weight Path
Route Distinguisher: 100:1 (Default for VRF 1)
[O]*> 1.1.1.1/32   10.1.1.1         2    32768 ?
[B]*>i2.2.2.2/32   22.22.22.22      0  100  0 200 ?
[O]*> 10.1.1.0/24  0.0.0.0          1    32768 ?
[B]*>i10.1.5.0/24  22.22.22.22      0  100  0 200 ?
```

```
ASBR1#show ip bgp vpnv4 all
BGP table version is 364, local router ID is 22.22.22.22
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
                S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop        Metric LocPrf Weight Path
Route Distinguisher: 100:1
[B]*>i1.1.1.1/32   11.11.11.11      2  100  0 ?
[B]*> 2.2.2.2/32   10.1.3.2          0    0 200 ?
[B]*>i10.1.1.0/24  11.11.11.11      1  100  0 ?
[B]*> 10.1.5.0/24  10.1.3.2          0    0 200 ?
```

It is indicated the BGP routing information to the peer CE2 exists in the BGP VPNv4 routing table of PE1 and ASBR1.

# View the route label table entries and MPLS forwarding table on PE and ASBR.

Take PE1, ASBR1 as an example.

```
PE1#show ip route vrf 1 2.2.2.2 detail
```

Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS

U - Per-user Static route

O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

```
B 2.2.2.2/32 [200/0] via 22.22.22.22, label 20480, 01:04:26, vlan3
    10.1.2.2 [2], label 3, vlan3
```

PE1#show mpls forwarding-table

Pro: L - LDP, B - MP-BGP, R - RSVP, M - Mapped-Route, ML - mLDP (ML FEC: Root address/OT/OV), RM - RSVP P2MP (RM FEC: P2MP ID/TID)

S - Static Label

Pro Ident	FEC	Inlabel	Outlabel	Outgoing	Next hop
B 1	0.0.0.0/0	5120	/	/	/

ASBR1#show mpls forwarding-table

Pro: L - LDP, B - MP-BGP, R - RSVP, M - Mapped-Route, ML - mLDP (ML FEC: Root address/OT/OV), RM - RSVP P2MP (RM FEC: P2MP ID/TID)

S - Static Label

Pro Ident	FEC	Inlabel	Outlabel	Outgoing	Next hop
B global	2.2.2.2/32	20480	16	vlan3	10.1.3.2
B global	10.1.5.0/24	20481	17	vlan3	10.1.3.2
B global	1.1.1.1/32	20482	5120	vlan2	11.11.11.11
B global	10.1.1.0/24	20483	5120	vlan2	11.11.11.11

It is indicated that the route label information of VPN1 exists in the forwarding table of PE1 and ASBR1.

---

## Note

- Refer to PE1 and ASBR1 for the inspection method of PE2 and ASBR2.
- 

#View the routing table on the CE.

Take CE1 as an example.

CE1#show ip route

Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS

U - Per-user Static route

O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

```
LC 1.1.1.1/32 is directly connected, 22:18:15, loopback0
O 2.2.2.2/32 [110/2] via 10.1.1.2, 00:35:47, vlan2
C 10.1.1.0/24 is directly connected, 22:22:30, vlan2
L 10.1.1.1/24 is directly connected, 22:22:30, vlan2
O 10.1.5.0/24 [110/2] via 10.1.1.2, 00:35:47, vlan2
C 127.0.0.0/8 is directly connected, 160:36:07, lo0
L 127.0.0.1/32 is directly connected, 160:36:07, lo0
```

It is indicated that the routing information to the peer CE2 exists in the CE1 routing table.

#Ping the loopback port of CE2 on CE1 to see if it can ping through properly.

```
CE1#ping 2.2.2.2
```

```
Press key (ctrl + shift + 6) interrupt it.
```

```
Sending 5, 76-byte ICMP Echos to 2.2.2.2 , timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100% (5/5). Round-trip min/avg/max = 0/0/0 ms.
```

It is indicated that CE1 can ping through to CE2.

### 79.3.5 Configure the AS replacement function of BGP.

#### Network Requirements

- Configure the MPLS L3VPN intra-domain environment.
- Both CE1 and CE2 are VPN1 devices.
- Both CE1 and CE2 belong to AS 100 and use EBGP to advertise routes to the PEs. Configure AS override to ensure that the CEs at both ends can receive routes from the other end normally.

#### Network Topology

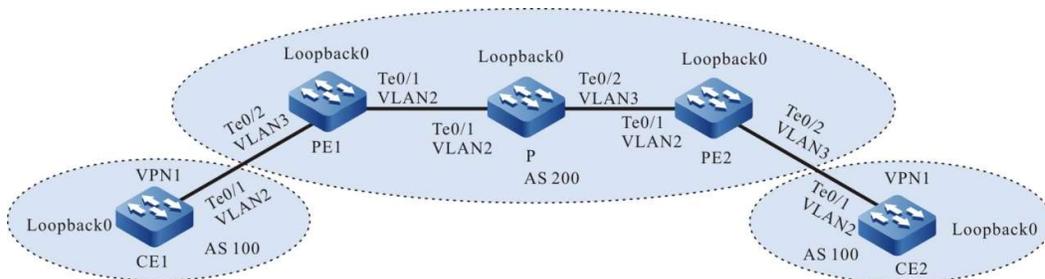


Figure 17-18 Network Topology for Configuring AS Replacement Function of BGP

Table 79-42 Interface Mapping Relationships

of equipment	Interface	IP address	of equipment	Interface	IP address
CE1	Vlan2	95.1.1.2/16	P	Loopback0	11.11.11.11/32
	Loopback0	5.5.5.5/32	PE2	Vlan2	92.1.1.1/16
PE1	Vlan2	93.1.1.2/16		Vlan3	90.1.1.1/16
	Vlan3	95.1.1.1/16		Loopback0	75.75.75.75/32
	Loopback0	90.90.90.90/32	CE2	Vlan2	90.1.1.2/16
P	Vlan2	93.1.1.1/16		Loopback0	8.8.8.8/32
	Vlan3	92.1.1.2/16			

### Configuration Steps

- Step 1: Configure the VLAN and add the port to the corresponding VLAN in access mode. (Omitted)
- Step 2: Configure IP addresses for the ports. (Omitted)
- Step 3: Configure global OSPF to advertise global routes.

#Configure global OSPF on PE1.

```

PE1#configure terminal
PE1(config)#router ospf 100
PE1(config-ospf)#network 90.90.90.90 0.0.0.0 area 0
PE1(config-ospf)#network 93.1.0.0 0.0.255.255 area 0
PE1(config-ospf)#exit

```

# Configure global OSPF on P.  
 User manual  
 Release 1.0 01/2022

```
P#configure terminal
P(config)#router ospf 100
P(config-ospf)#network 11.11.11.11 0.0.0.0 area 0
P(config-ospf)#network 92.1.0.0 0.0.255.255 area 0
P(config-ospf)#network 93.1.0.0 0.0.255.255 area 0
P(config-ospf)#exit
```

#Configure global OSPF on PE2.

```
PE2#configure terminal
PE2(config)#router ospf 100
PE2(config-ospf)#network 75.75.75.75 0.0.0.0 area 0
PE2(config-ospf)#network 92.1.0.0 0.0.255.255 area 0
PE2(config-ospf)#exit
```

#After the configuration is complete, view the global routing table on the device.

Take PE1 as an example:

```
PE1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

O 11.11.11.11/32 [110/2] via 93.1.1.1, 00:05:03, vlan2
O 75.75.75.75/32 [110/3] via 93.1.1.1, 00:06:03, vlan2
LC 90.90.90.90/32 is directly connected, 154:02:28, loopback0
O 92.1.0.0/16 [110/2] via 93.1.1.1, 00:08:12, vlan2
C 93.1.0.0/16 is directly connected, 00:34:54, vlan2
L 93.1.1.2/32 is directly connected, 00:34:54, vlan2
```

It is indicated the routing information of the loopback port of P and PE2 exists in the global routing table of PE1.

---

## Note

- Refer to PE1 for the inspection method of P and PE2.
-

Step 4: Enable MPLS IP and MPLS LDP.

#Enable global MPLS IP and MPLS LDP on PE1, and also enable MPLS IP and MPLS LDP on the interface.

```
PE1(config)#mpls ip
PE1(config)#mpls ldp
PE1(config-ldp)#router-id 90.90.90.90
PE1(config-ldp)#address-family ipv4
PE1(config-ldp-af4)#transport-address 90.90.90.90
PE1(config-ldp-af4)#exit
PE1(config-ldp)#exit
PE1(config)#interface vlan2
PE1(config-if-vlan2)#mpls ip
PE1(config-if-vlan2)#mpls ldp
PE1(config-if-vlan2)#exit
```

# Enable global MPLS IP and MPLS LDP on P. Also enable MPLS IP and MPLS LDP on the interface.

```
P(config)#mpls ip
P(config)#mpls ldp
P(config-ldp)#router-id 11.11.11.11
P(config-ldp)#address-family ipv4
P(config-ldp-af4)#transport-address 11.11.11.11
P(config-ldp-af4)#exit
P(config-ldp)#exit
P(config)#interface vlan2
P(config-if-vlan2)#mpls ip
P(config-if-vlan2)#mpls ldp
P(config-if-vlan2)#exit
P(config)#interface vlan3
P(config-if-vlan3)#mpls ip
P(config-if-vlan3)#mpls ldp
P(config-if-vlan3)#exit
```

# Enable global MPLS IP and MPLS LDP on PE2, and also enable MPLS IP and MPLS LDP on the interface.

```
PE2(config)#mpls ip
PE2(config)#mpls ldp
PE2(config-ldp)#router-id 75.75.75.75
PE2(config-ldp)#address-family ipv4
PE2(config-ldp-af4)#transport-address 75.75.75.75
PE2(config-ldp-af4)#exit
PE2(config-ldp)#exit
PE2(config)#interface vlan2
```

```
PE2(config-if-vlan2)#mpls ip
PE2(config-if-vlan2)#mpls ldp
PE2(config-if-vlan2)#exit
```

# After the configuration is complete, view the LDP session information on the device.

Take PE1 as an example:

```
PE1#show mpls ldp session
Peer IP Address Peer Type My Role State DS Cap DeadTime
11.11.11.11 Multicast Active OPERATIONAL Disabled 00:02:20
Statistics for ldp sessions:
Multicast sessions: 1
Targeted sessions: 0
```

It is indicated that PE1 successfully establishes an LDP session with P.

#View the routing label table entries on the device.

Take PE1 as an example:

```
PE1#show ip route 11.11.11.11 detail
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
U - Per-user Static route
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
O 11.11.11.11/32 [110/2] via 93.1.1.1, label 3, 14:29:21, vlan2
93.1.1.1 [0], vlan2
```

```
PE1#show ip route 75.75.75.75 detail
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
U - Per-user Static route
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
O 75.75.75.75/32 [110/3] via 93.1.1.1, label 16, 14:30:21, vlan2
93.1.1.1 [0], vlan2
```

It is indicated the label information of the loopback ports to P and PE2 exist on PE1.

---

 **Note**

- Refer to PE1 for the inspection method of P and PE2.
- 

Step 5: Configure a VPN instance on the PE and configure BGP between the PE and the CE.

#Configure VPN instance on PE1 and establish EBGP neighbor with CE.

```
PE1(config)#ip vrf 1
PE1(config-vrf)#rd 100:1
PE1(config-vrf)#route-target export 100:1
PE1(config-vrf)#route-target import 100:1
PE1(config-vrf)#exit
PE1(config)#interface vlan3
PE1(config-if-vlan3)#ip vrf forwarding 1
PE1(config-if-vlan3)#ip address 95.1.1.1 255.255.0.0
PE1(config-if-vlan3)#exit
PE1(config)#router bgp 200
PE1(config-bgp)#address-family ipv4 vrf 1
PE1(config-bgp-af)#neighbor 95.1.1.2 remote-as 100
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
```

#Configure EBGP with PE on CE1.

```
CE1#configure terminal
CE1(config)#router bgp 100
CE1(config-bgp)#network 5.5.5.5 255.255.255.255
CE1(config-bgp)#network 95.1.0.0 255.255.0.0
CE1(config-bgp)#neighbor 95.1.1.1 remote-as 200
CE1(config-bgp)#exit
```

#Configure VPN instance on PE2 and establish EBGP neighbor with CE.

```
PE2(config)#ip vrf 1
PE2(config-vrf)#rd 100:1
PE2(config-vrf)#route-target export 100:1
PE2(config-vrf)#route-target import 100:1
PE2(config-vrf)#exit
PE2(config)#interface vlan3
PE2(config-if-vlan3)#ip vrf forwarding 1
PE2(config-if-vlan3)#ip address 90.1.1.1 255.255.0.0
```

```

PE2(config-if-vlan3)#exit
PE2(config)#router bgp 200
PE2(config-bgp)#address-family ipv4 vrf 1
PE2(config-bgp-af)#neighbor 90.1.1.2 remote-as 100
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#exit

```

#Configure EBGP with PE on CE2.

```

CE2#configure terminal
CE2(config)#router bgp 100
CE2(config-bgp)#network 8.8.8.8 255.255.255.255
CE2(config-bgp)#network 90.1.0.0 255.255.0.0
CE2(config-bgp)#neighbor 90.1.1.1 remote-as 200
CE2(config-bgp)#exit

```

# After the configuration is complete, check the EBGP neighbor information on the PE.

Take PE1 as an example:

```

PE1#show ip bgp vpnv4 all summary
BGP router identifier 90.90.90.90, local AS number 200BGP VRF 1 Route Distinguisher:
100:1
BGP table version is 1
1 BGP AS-PATH entries
0 BGP community entries

```

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
95.1.1.2	4	100	2	2	1	0	00:00:08	2	

Total number of neighbors 1

The successful establishment of BGP neighbors between PE1 and CE1 can be seen from the fact that the contents of the column State/PfxRcd are shown as numbers (the number of received route prefixes from neighbors).

#View the BGP VPNv4 routing table and VPN routing table on the PE.

```

PE1#show ip bgp vpnv4 vrf 1
BGP table version is 18, local router ID is 90.90.90.90
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
                S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Network        Next Hop        Metric LocPrf Weight Path
Route Distinguisher: 100:1 (Default for VRF 1)
[B]*> 5.5.5.5/32    95.1.1.2        0        0 100 i

```

```
[B]*> 95.1.0.0/16    95.1.1.2        0        0 100 i
```

```
PE1#show ip route vrf 1
```

```
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
```

```
U - Per-user Static route
```

```
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
B 5.5.5.5/32 [20/0] via 95.1.1.2, 01:13:15, vlan3 .
```

```
C 95.1.0.0/16 is directly connected, 15:40:01, vlan3
```

```
L 95.1.1.1/32 is directly connected, 15:40:01, vlan3
```

It is indicated that routes to CE1 exist in the BGP routing table and VPN routing table of PE1.

---

 **Note**

- Refer to PE1 for the inspection method of PE2.
- 

Step 6: Configure the MP-IBGP to use the loopback interface as the peer address.

#Configure MP-IBGP on PE1 and enable VPNv4 address clustering.

```
PE1(config)#router bgp 200
PE1(config-bgp)#neighbor 75.75.75.75 remote-as 200
PE1(config-bgp)#neighbor 75.75.75.75 update-source loopback0
PE1(config-bgp)#address-family vpnv4
PE1(config-bgp-af)#neighbor 75.75.75.75 activate
PE1(config-bgp-af)#neighbor 75.75.75.75 send-community extended
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
```

#Configure MP-IBGP on PE2 and enable VPNv4 address clustering.

```
PE2(config)#router bgp 200
PE2(config-bgp)#neighbor 90.90.90.90 remote-as 200
PE2(config-bgp)#neighbor 90.90.90.90 update-source loopback0
PE2(config-bgp)#address-family vpnv4
PE2(config-bgp-af)#neighbor 90.90.90.90 activate
PE2(config-bgp-af)#neighbor 90.90.90.90 send-community extended
```

```
PE2(config-bgp-af)#exit-address-family
```

```
PE2(config-bgp)#exit
```

# After the configuration is complete, view the BGP neighbor information on the PE.

Take PE1 as an example:

```
PE1#show ip bgp vpnv4 all summary
```

```
BGP router identifier 90.90.90.90, local AS number 200
```

```
BGP table version is 2
```

```
1 BGP AS-PATH entries
```

```
0 BGP community entries
```

```
Neighbor    V  AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down State/PfxRcd
75.75.75.75 4 200    3     3    1  0  0 00:00:06    4
```

```
Total number of neighbors 1
```

```
BGP VRF 1 Route Distinguisher:
```

```
100:1
```

```
BGP table version is 1
```

```
2 BGP AS-PATH entries
```

```
0 BGP community entries
```

```
Neighbor    V  AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down State/PfxRcd
95.1.1.2    4 100   18    18    1  0  0 00:14:25    2
```

```
Total number of neighbors 1
```

The successful establishment of BGP neighbors between PE1 and PE2 and CE1 can be seen from the fact that the contents of the column State/PfxRcd are shown as numbers (the number of received route prefixes from neighbors).

#View the BGP VPNv4 routing table and VPN routing table on the PE.

Take PE1 as an example:

```
PE1#show ip bgp vpnv4 vrf 1
```

```
BGP table version is 27, local router ID is 90.90.90.90
```

```
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
```

```
S Stale
```

```
Origin codes: i - IGP, e - EGP, ? - incomplete
```

```
Network      Next Hop      Metric LocPrf Weight Path
```

```
Route Distinguisher: 100:1 (Default for VRF 1)
```

```
[B]*> 5.5.5.5/32    95.1.1.2      0      0 100 i
```

```
[B]*> 8.8.8.8/32    75.75.75.75   0 100  0 100 i
```

```
[B]*>90.1.0.0/16    75.75.75.75      0 100  0 100 i
[B]*> 95.1.0.0/16    95.1.1.2         0      0 100 i
```

```
PE1#show ip bgp vpnv4 vrf 1 8.8.8.8
```

```
Route Distinguisher: 100:1 (Default for VRF 1), Prefix: 8.8.8.8/32
```

```
Not advertised to any peer
```

```
100
```

```
75.75.75.75 (metric 3) from 75.75.75.75 (75.75.75.75)
```

```
Origin IGP, metric 0, localpref 100, valid, internal, best, vrf fn installed, vrf duplicated, vrf external
```

```
Extended Community: RT:100:1
```

```
Last update: 01:38:32 ago
```

```
PE1#show ip route vrf 1
```

```
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
```

```
U - Per-user Static route
```

```
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
B 5.5.5.5/32 [20/0] via 95.1.1.2, 00:09:40, vlan3
```

```
B 8.8.8.8/32 [200/0] via 75.75.75.75, 01:46:03, vlan2
```

```
B 90.1.0.0/16 [200/0] via 75.75.75.75, 00:04:05, vlan2
```

```
C 95.1.0.0/16 is directly connected, 18:33:25, vlan3
```

```
L 95.1.1.1/32 is directly connected, 18:33:25, vlan3
```

It is indicated that the routing information to CE2 exists in the BGP VPNv4 routing table of PE1, and the AS-PATH shows 100, and the routing information to CE2 also exists in the VPN1 routing table of PE1.

---

## Note

- Refer to PE1 for the inspection method of PE2.
- 

#View the BGP routing table on the CE.

Take CE1 as an example.

```
CE1#show ip bgp
```

```
BGP table version is 1, local router ID is 5.5.5.5
```

Status codes: s suppressed, d damped, h history, \* valid, > best, i - internal,

S Stale

Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
[B]*> 5.5.5.5/32	0.0.0.0	0	32768	i	
[B]*> 95.1.0.0/16	0.0.0.0	0	32768	i	

You can find that there is no route information to CE2 in the BGP routing table of CE1.

---

## Note

- Since CE finds that the AS PATH attribute of the received peer route contains the same AS number 100 as its own, it rejects the BGP route. Configuration is needed for AS override on the PE before the CE can learn the peer route.
- 

Step 7: Configure AS override on the PE.

#Configure AS override function for EBGP neighbors under the BGP VRF address cluster of PE1, so that the AS number same as the CE is communicated to the CE as its own local AS number.

```
PE1(config)#router bgp 200
PE1(config-bgp)#address-family ipv4 vrf 1
PE1(config-bgp-af)#neighbor 95.1.1.2 as-override
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
```

#Configure AS override for EBGP neighbors under the BGP VRF address cluster of PE2, thus overriding the AS number same as the CE as its own local AS number to pass to the CE.

```
PE2(config)#router bgp 200
PE2(config-bgp)#address-family ipv4 vrf 1
PE2(config-bgp-af)#neighbor 90.1.1.2 as-override
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#exit
```

Step 8: Check the result.

#After the configuration is complete, view the BGP VPNv4 routing table and VPN routing table on the PE.

Take PE1 as an example:

```
PE1#show ip bgp vpnv4 vrf 1
BGP table version is 27, local router ID is 90.90.90.90
```

Status codes: s suppressed, d damped, h history, \* valid, > best, i - internal,

S Stale

Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
Route Distinguisher: 100:1 (Default for VRF 1)					
[B]*> 5.5.5.5/32	95.1.1.2	0	0	100	i
[B]*>i8.8.8.8/32	75.75.75.75	0	100	0	100 i
[B]*>i90.1.0.0/16	75.75.75.75	0	100	0	100 i
[B]*> 95.1.0.0/16	95.1.1.2	0	0	100	i

PE1#show ip bgp vpnv4 vrf 1 8.8.8.8

Route Distinguisher: 100:1 (Default for VRF 1), Prefix: 8.8.8.8/32

Not advertised to any peer

100

75.75.75.75 (metric 3) from 75.75.75.75 (75.75.75.75)

Origin IGP, metric 0, localpref 100, valid, internal, best, vrf ftm installed, vrf duplicated, vrf external

Extended Community: RT:100:1

Last update: 01:38:32 ago

PE1#show ip route vrf 1

Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS

U - Per-user Static route

O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

B 5.5.5.5/32 [20/0] via 95.1.1.2, 00:09:40, vlan3  
B 8.8.8.8/32 [200/0] via 75.75.75.75, 01:46:03, vlan2  
B 90.1.0.0/16 [200/0] via 75.75.75.75, 00:04:05, vlan2  
C 95.1.0.0/16 is directly connected, 18:33:25, vlan3  
L 95.1.1.1/32 is directly connected, 18:33:25, vlan3

It is indicated that the routing information to CE2 exists in the BGP VPNv4 routing table of PE1, and the AS-PATH shows 100, and the routing information to CE2 also exists in the VPN1 routing table of PE1.

#View the BGP routing table again on the CE.

CE1#show ip bgp

BGP table version is 4, local router ID is 5.5.5.5

Status codes: s suppressed, d damped, h history, \* valid, > best, i - internal,

S Stale

Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
[B]*> 5.5.5.5/32	0.0.0.0	0	32768	i	
[B]*> 8.8.8.8/32	95.1.1.1	0	0 200 200	i	
[B]*> 90.1.0.0/16	95.1.1.1	0	0 200 200	i	
[B]*> 95.1.0.0/16	0.0.0.0	0	32768	i	

CE1#show ip bgp 8.8.8.8

BGP routing table entry for 8.8.8.8/32

Paths: (1 available, best #1, table Default-IP-Routing-Table)

Not advertised to any peer

200 200

95.1.1.1 (metric 100) from 95.1.1.1 (90.90.90.90)

Origin IGP, metric 0, localpref 100, valid, external, best

Last update: 00:06:06 ago

CE1#show ip route

Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS

U - Per-user Static route

O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

LC 5.5.5.5/32 is directly connected, 04:05:46, loopback0

B 8.8.8.8/32 [20/0] via 95.1.1.1, 00:08:51, vlan2

B 90.1.0.0/16 [20/0] via 95.1.1.1, 00:03:09, vlan2

C 95.1.0.0/16 is directly connected, 23:33:15, vlan2

L 95.1.1.2/32 is directly connected, 23:33:15, vlan2

It is indicated that the route information to CE2 exists in both the BGP routing table and the global routing table of CE1, and it is indicated that the AS-PATH of the route to CE2 is modified to 200 200 in the BGP routing table.

Ping the loopback port of CE2 on CE1 and see if it pings through.

CE1#ping 8.8.8.8

Press key (ctrl + shift + 6) interrupt it.

Sending 5, 76-byte ICMP Echos to 8.8.8.8 , timeout is 2 seconds:

!!!!

Success rate is 100% (5/5). Round-trip min/avg/max = 0/0/0 ms.

It is indicated that CE1 can ping through CE2.

### 79.3.6 Configure OSPF pseudo-Connections

#### Network Requirements

- CE1 and CE2 belong to VPN1, and OSPF for route advertisement is used between CE and PE.
- A backdoor link exists between CE1 and CE2. Configure pseudo-connections between PEs so that VPN traffic between CE1 and CE2 is forwarded globally via MPLS on a priority basis, using only the backdoor link for backup.
- Configure OSPF between PEs to achieve intra-PE communication and configure MP-IBGP to exchange VPN routing information.

#### Network Topology

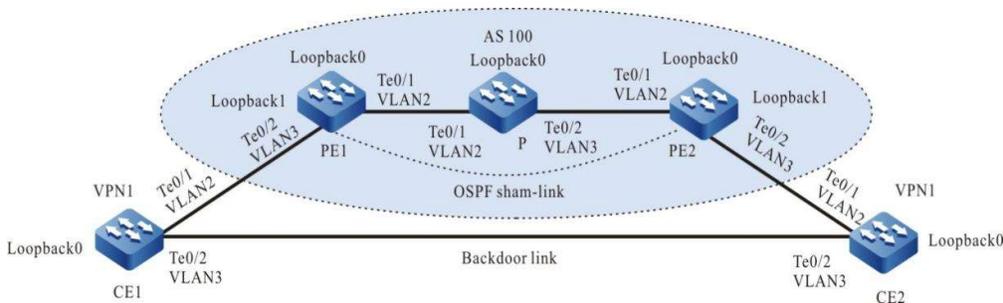


Figure 19-20 Network Topology for Configuring an OSPF Pseudo-Link

Table 43-44 Interface Mapping Relationships

of equipment	Interface	IP address	of equipment	Interface	IP address
CE1	Vlan2	95.1.1.2/16	P	Loopback0	11.11.11.11/32
	Vlan3	98.1.1.1/16	PE2	Vlan2	92.1.1.1/16
	Loopback0	5.5.5.5/32		Vlan3	90.1.1.1/16
PE1	Vlan2	93.1.1.2/16		Loopback0	75.75.75.75/32
	Vlan3	95.1.1.1/16		Loopback1	6.6.6.6/32
	Loopback0	90.90.90.90/32	CE2	Vlan2	90.1.1.2/16

of equipment	Interface	IP address	of equipment	Interface	IP address
	Loopback1	1.1.1.1/32		Vlan3	98.1.1.2/16
P	Vlan2	93.1.1.1/16		Loopback0	8.8.8.8/32
	Vlan3	92.1.1.2/16			

### Configuration Steps

Step 1: Configure the VLAN and add the port to the corresponding VLAN in access mode.  
(Omitted)

Step 2: Configure IP addresses for the ports. (Omitted)

Step 3: Configure global OSPF to advertise global routes.

#Configure global OSPF on PE1.

```
PE1#configure terminal
PE1(config)#router ospf 100
PE1(config-ospf)#network 90.90.90.90 0.0.0.0 area 0
PE1(config-ospf)#network 93.1.0.0 0.0.255.255 area 0
PE1(config-ospf)#exit
```

# Configure global OSPF on P.

```
P#configure terminal
P(config)#router ospf 100
P(config-ospf)#network 11.11.11.11 0.0.0.0 area 0
P(config-ospf)#network 92.1.0.0 0.0.255.255 area 0
P(config-ospf)#network 93.1.0.0 0.0.255.255 area 0
P(config-ospf)#exit
```

#Configure global OSPF on PE2's.

```
PE2#configure terminal
PE2(config)#router ospf 100
PE2(config-ospf)#network 75.75.75.75 0.0.0.0 area 0
PE2(config-ospf)#network 92.1.0.0 0.0.255.255 area 0
PE2(config-ospf)#exit
```

#After the configuration is complete, view the global routing table on the device.

Take PE1 as an example:

```
PE1#show ip route
```

Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS

U - Per-user Static route

O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

```
O 11.11.11.11/32 [110/2] via 93.1.1.1, 00:05:03, vlan2
O 75.75.75.75/32 [110/3] via 93.1.1.1, 00:06:03, vlan2
LC 90.90.90.90/32 is directly connected, 00:08:28, loopback0
O 92.1.0.0/16 [110/2] via 93.1.1.1, 00:08:12, vlan2
C 93.1.0.0/16 is directly connected, 00:34:54, vlan2
L 93.1.1.2/32 is directly connected, 00:34:54, vlan2
```

It is indicated that the routing information of PE2 and P's loopback port exists in the global routing table of PE1.

---

## Note

- Refer to PE1 for the inspection method of P and PE2.
- 

Step 4: Enable MPLS IP and MPLS LDP.

#Enable global MPLS IP and MPLS LDP on PE1, and also enable MPLS IP and MPLS LDP on the interface.

```
PE1(config)#mpls ip
PE1(config)#mpls ldp
PE1(config-ldp)#router-id 90.90.90.90
PE1(config-ldp)#address-family ipv4
PE1(config-ldp-af4)#transport-address 90.90.90.90
PE1(config-ldp-af4)#exit
PE1(config-ldp)#exit
PE1(config)#interface vlan2
PE1(config-if-vlan2)#mpls ip
PE1(config-if-vlan2)#mpls ldp
PE1(config-if-vlan2)#exit
```

# Enable global MPLS IP and MPLS LDP on P. Also enable MPLS IP and MPLS LDP on the interface.

```
P(config)#mpls ip
P(config)#mpls ldp
```

```

P(config-ldp)#router-id 11.11.11.11
P(config-ldp)#address-family ipv4
P(config-ldp-af4)#transport-address 11.11.11.11
P(config-ldp-af4)#exit
P(config-ldp)#exit
P(config)#interface vlan2
P(config-if-vlan2)#mpls ip
P(config-if-vlan2)#mpls ldp
P(config-if-vlan2)#exit
P(config)#interface vlan3
P(config-if-vlan3)#mpls ip
P(config-if-vlan3)#mpls ldp
P(config-if-vlan3)#exit

```

# Enable global MPLS IP and MPLS LDP on PE2, and also enable MPLS IP and MPLS LDP on the interface.

```

PE2(config)#mpls ip
PE2(config)#mpls ldp
PE2(config-ldp)#router-id 75.75.75.75
PE2(config-ldp)#address-family ipv4
PE2(config-ldp-af4)#transport-address 75.75.75.75
PE2(config-ldp-af4)#exit
PE2(config-ldp)#exit
PE2(config)#interface vlan2
PE2(config-if-vlan2)#mpls ip
PE2(config-if-vlan2)#mpls ldp
PE2(config-if-vlan2)#exit

```

# After the configuration is complete, view the LDP session information on the device.

Take PE1 as an example:

```

PE1#show mpls ldp session
Peer IP Address  Peer Type  My Role  State    DS Cap  DeadTime
11.11.11.11     Multicast  Active   OPERATIONAL  Disabled 00:02:20
Statistics for ldp sessions:
  Multicast sessions: 1
  Targeted sessions: 0

```

It is indicated that PE1 successfully establishes an LDP session with P.

#View the routing label table entries on the device.

Take PE1 as an example:

```

PE1#show ip route 11.11.11.11 detail

```

Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS

U - Per-user Static route

O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

```
O 11.11.11.11/32 [110/2] via 93.1.1.1, label 3, 14:29:21, vlan2
    93.1.1.1 [0], vlan2
```

```
PE1#show ip route 75.75.75.75 detail
```

Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS

U - Per-user Static route

O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

```
O 75.75.75.75/32 [110/3] via 93.1.1.1, label 16, 14:30:21, vlan2
    93.1.1.1 [0], vlan2
```

It is indicated the label information of the loopback ports to P and PE2 exist on PE1.

---

## Note

- Refer to PE1 for the inspection method of P and PE2.
- 

Step 5: Configure the VPN instance to advertise the CE route to the PE via OSPF.

#Configure VPN instance and OSPF under VPN instance on PE1.

```
PE1(config)#ip vrf 1
PE1(config-vrf)#rd 100:1
PE1(config-vrf)#route-target export 100:1
PE1(config-vrf)#route-target import 100:1
PE1(config-vrf)#exit
PE1(config)#interface vlan3
PE1(config-if-vlan3)#ip vrf forwarding 1
PE1(config-if-vlan3)#ip address 95.1.1.1 255.255.0.0
PE1(config-if-vlan3)#exit
```

```
PE1(config)#router ospf 200 vrf 1
PE1(config-ospf)#network 95.1.0.0 0.0.255.255 area 0
PE1(config-ospf)#exit
```

#Configure OSPF between CE1 and PE1 and CE2 on CE1.

```
CE1#configure terminal
CE1(config)#router ospf 100
CE1(config-ospf)#network 5.5.5.5 0.0.0.0 area 0
CE1(config-ospf)#network 95.1.0.0 0.0.255.255 area 0
CE1(config-ospf)#network 98.1.0.0 0.0.255.255 area 0
CE1(config-ospf)#exit
```

#Configure VPN instance and OSPF under VPN instance on PE2.

```
PE2(config)#ip vrf 1
PE2(config-vrf)#rd 100:1
PE2(config-vrf)#route-target export 100:1
PE2(config-vrf)#route-target import 100:1
PE2(config-vrf)#exit
PE2(config)#interface vlan3
PE2(config-if-vlan3)#ip vrf forwarding 1
PE2(config-if-vlan3)#ip address 90.1.1.1 255.255.0.0
PE2(config-if-vlan3)#exit
PE2(config)#router ospf 200 vrf 1
PE2(config-ospf)#network 90.1.0.0 0.0.255.255 area 0
PE2(config-ospf)#exit
```

#Configure OSPF on CE2 with PE2 and CE1.

```
CE2#configure terminal
CE2(config)#router ospf 100
CE2(config-ospf)#network 8.8.8.8 0.0.0.0 area 0
CE2(config-ospf)#network 90.1.0.0 0.0.255.255 area 0
CE2(config-ospf)#network 98.1.0.0 0.0.255.255 area 0
CE2(config-ospf)#exit
```

#After the configuration is complete, view the VPN routing table on the PE.

Take PE1 as an example:

```
PE1#show ip route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

- O 5.5.5.5/32 [110/2] via 95.1.1.2, 00:11:11, vlan3
- C 95.1.0.0/16 is directly connected, 00:11:45, vlan3
- L 95.1.1.1/32 is directly connected, 00:11:45, vlan3
- O 98.1.0.0/16 [110/2] via 95.1.1.2, 00:10:11, vlan3

It is indicated the loopback port routing information to CE1 exists in the VPN routing table of PE1.

---

 **Note**

- Refer to PE1 for the inspection method of PE2.
- 

Step 6: Configure the MP-IBGP to use the loopback interface as the peer address; and redistribute routes with each other and the IGP protocol under the VPN instance.

#Configure the MP-IBGP on PE1 to enable VPNv4 address clustering; and redistribute routes with each other and the IGP protocol under the VPN instance.

```
PE1(config)#router bgp 100
PE1(config-bgp)#neighbor 75.75.75.75 remote-as 100
PE1(config-bgp)#neighbor 75.75.75.75 update-source loopback0
PE1(config-bgp)#address-family vpnv4
PE1(config-bgp-af)#neighbor 75.75.75.75 activate
PE1(config-bgp-af)#neighbor 75.75.75.75 send-community extended
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#address-family ipv4 vrf 1
PE1(config-bgp-af)#redistribute ospf 200
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
PE1(config)#router ospf 200 vrf 1
PE1(config-ospf)#redistribute bgp 100
PE1(config-ospf)#exit
```

#Configure the MP-IBGP on PE2 to enable VPNv4 address clustering; and redistribute routes with each other and the IGP protocol under the VPN instance.

```
PE2(config)#router bgp 100
PE2(config-bgp)#neighbor 90.90.90.90 remote-as 100
PE2(config-bgp)#neighbor 90.90.90.90 update-source loopback0
PE2(config-bgp)#address-family vpnv4
```

```

PE2(config-bgp-af)#neighbor 90.90.90.90 activate
PE2(config-bgp-af)#neighbor 90.90.90.90 send-community extended
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#address-family ipv4 vrf 1
PE2(config-bgp-af)#redistribute ospf 200
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#exit
PE2(config)#router ospf 200 vrf 1
PE2(config-ospf)#redistribute bgp 100
PE2(config-ospf)#exit

```

# After the configuration is completed, check the BGP neighbor information on PE1.

Take PE1 as an example:

```

PE1#show ip bgp vpnv4 all summary
BGP router identifier 90.90.90.90, local AS number 100
BGP table version is 6
1 BGP AS-PATH entries
0 BGP community entries

Neighbor    V  AS MsgRcvd MsgSent  TblVer  InQ  OutQ  Up/Down  State/PfxRcd
75.75.75.75  4 100   40   41     5   0  00:32:01    2

Total number of neighbors 1

```

The successful establishment of BGP neighbors between PE1 and PE2 can be seen from the fact that the contents of the column State/PfxRcd are shown as numbers (the number of received route prefixes from neighbors).

#View the BGP VPNv4 routing table and VPN routing table on the PE.

Take PE1 as an example:

```

PE1#show ip bgp vpnv4 vrf 1
BGP table version is 19, local router ID is 90.90.90.90
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Network      Next Hop      Metric LocPrf Weight Path
Route Distinguisher: 100:1 (Default for VRF 1)
[B]* i5.5.5/32    75.75.75.75    5 100  0 ?
[O]*>          95.1.1.2       2  32768 ?
[O]*> 8.8.8/32    95.1.1.2       5  32768 ?
[B]* i          75.75.75.75    2 100  0 ?

```

```

[O]*> 90.1.0.0/16    95.1.1.2        5    32768 ?
[B]* i          75.75.75.75    1 100  0 ?
[B]* i95.1.0.0/16    75.75.75.75    5 100  0 ?
[O]*>          0.0.0.0         1    32768 ?
[B]* i98.1.0.0/16    75.75.75.75    4 100  0 ?
[O]*>          95.1.1.2        4    32768 ?

```

```
PE1#show ip route vrf 1
```

```
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
```

```
U - Per-user Static route
```

```
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```

O 5.5.5.5/32 [110/2] via 95.1.1.2, 03:00:43, vlan3
O 8.8.8.8/32 [110/5] via 95.1.1.2, 00:00:05, vlan3
O 90.1.0.0/16 [110/5] via 95.1.1.2, 00:00:05, vlan3
C 95.1.0.0/16 is directly connected, 03:01:34, vlan3
L 95.1.1.1/32 is directly connected, 03:01:34, vlan3
O 98.1.0.0/16 [110/4] via 95.1.1.2, 02:58:04, vlan3

```

It is indicated that the routes to CE2 in the BGP VPNv4 routing table and VPN routing table are through the backdoor link of CE1, not through the global MPLS network.

---

## Note

- Refer to PE1 for the inspection method of PE2.
- 

Step 7: Configure OSPF pseudo-connections on the PE and configure the COST value of the interface on the CE1 backdoor link to enable communication between CEs over the global network.

#Configure OSPF pseudo-connections on PE1 and advertise the loopback port route of the OSPF pseudo-link initiation point in BGP.

```

PE1(config)#interface loopback 1
PE1(config-if-loopback1)#ip vrf forwarding 1
PE1(config-if-loopback1)#ip address 1.1.1.1 255.255.255.255
PE1(config-if-loopback1)#exit

```

```
PE1(config)#router bgp 100
PE1(config-bgp)#address-family ipv4 vrf 1
PE1(config-bgp-af)#network 1.1.1.1 255.255.255.255
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
PE1(config)#router ospf 200 vrf 1
PE1(config-ospf)#area 0 sham-link 1.1.1.1 6.6.6.6
PE1(config-ospf)#exit
```

# Configure OSPF pseudo-connections on PE2 and advertise the loopback port route of the OSPF pseudo-link initiation point in BGP.

```
PE2(config)#interface loopback 1
PE2(config-if-loopback1)#ip vrf forwarding 1
PE2(config-if-loopback1)#ip address 6.6.6.6 255.255.255.255
PE2(config-if-loopback1)#exit
PE2(config)#router bgp 100
PE2(config-bgp)#address-family ipv4 vrf 1
PE2(config-bgp-af)#network 6.6.6.6 255.255.255.255
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#exit
PE2(config)#router ospf 200 vrf 1
PE2(config-ospf)#area 0 sham-link 6.6.6.6 1.1.1.1
PE2(config-ospf)#exit
```

# Modify the COST value of the backdoor routing interface on CE1 to enable communication between CEs via the global

```
CE1(config)#interface vlan3
CE1(config-if-vlan3)#ip ospf cost 4
CE1(config-if-vlan3)#exit
```

# Modify the COST value of the backdoor routing interface on CE2 to enable global communication between CEs.

```
CE2(config)#interface vlan3
CE2(config-if-vlan3)#ip ospf cost 4
CE2(config-if-vlan3)#exit
```

Step 8: Check the result.

#After the configuration is complete, view the OSPF pseudo-connection information on the PE.

```
PE1#show ip ospf sham-links
Sham Link SLINK0 to addr 6.6.6.6 is up
Area 0.0.0.0 source address 1.1.1.1
```

```

Run as demand circuit
DoNotAge LSA allowed. Cost of using 1 State Point-To-Point,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:07
Adjacency state Full(Hello suppressed)

```

```

PE2#show ip ospf sham-links
Sham Link SLINK0 to addr 1.1.1.1 is up
Area 0.0.0.0 source address 6.6.6.6
Run as demand circuit
DoNotAge LSA allowed. Cost of using 1 State Point-To-Point,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:04
Adjacency state Full(Hello suppressed)

```

# Re-view the BGP VPNv4 routing table and VPN routing table on the PE.

Take PE1 as an example:

```

PE1#show ip route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
U - Per-user Static route
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

```

```

LC 1.1.1.1/32 is directly connected, 00:12:09, loopback1
O 5.5.5.5/32 [110/2] via 95.1.1.2, 03:21:34, vlan3
B 6.6.6.6/32 [200/0] via 75.75.75.75, 03:09:38, vlan2
O 8.8.8.8/32 [110/3] via 75.75.75.75, 00:11:32, vlan2
O 90.1.0.0/16 [110/2] via 75.75.75.75, 00:11:32, vlan2
C 95.1.0.0/16 is directly connected, 03:22:25, vlan3
L 95.1.1.1/32 is directly connected, 03:22:25, vlan3
O 98.1.0.0/16 [110/4] via 95.1.1.2, 03:18:55, vlan3

```

```

PE1#show ip bgp vpnv4 vrf 1
BGP table version is 17, local router ID is 90.90.90.90
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Network      Next Hop      Metric LocPrf Weight Path
Route Distinguisher: 100:1 (Default for VRF 1)
[B]*> 1.1.1.1/32    0.0.0.0      0    32768 i

```

```

[O]*> 5.5.5.5/32    95.1.1.2        2    32768 ?
[B]*>i6.6.6.6/32    75.75.75.75     0    100   0 i
[B]*>i8.8.8.8/32    75.75.75.75     2    100   0 ?
[B]*>i90.1.0.0/16   75.75.75.75     1    100   0 ?
[O]*> 95.1.0.0/16   0.0.0.0         1    32768 ?
[B]* i98.1.0.0/16   75.75.75.75     4    100   0 ?
[O]*>                95.1.1.2        4    32768 ?

```

It is indicated that the routes to CE2 in PE1's BGP VPNv4 routing table and VPN routing table are through the global MPLS network and not through CE1's backdoor link.

#View the routing label table entries and MPLS forwarding table entries on the PE.

Take PE1 as an example:

```

PE1#show ip route vrf 1 6.6.6.6 detail
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

```

```

B 6.6.6.6/32 [200/0] via 75.75.75.75, label 5120, 01:04:26, vlan2
    93.1.1.1 [3], label 16, vlan2

```

```

PE1#show ip route vrf 1 8.8.8.8 detail
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

```

```

O 8.8.8.8/32 [110/3] via 6.6.6.6, label 5120, 01:04:41, vlan2
    93.1.1.1 [3], label 16, vlan2

```

```

PE1#show mpls forwarding-table
Pro: L - LDP, B - MP-BGP, R - RSVP, M - Mapped-Route, ML - mLDP (ML FEC: Root
address/OT/OV), RM - RSVP P2MP (RM FEC: P2MP ID/TID)
S - Static Label

```

Pro	Ident	FEC	Inlabel	Outlabel	Outgoing	Next hop
B	1	0.0.0.0/0	5120	/	/	/

It is indicated that the route label information of VPN1 exists in the forwarding table of PE1.

---

## Note

- Refer to PE1 for the inspection method of PE2.
- 

# View VPN on CE1      Routing table, and traceroute CE2's loopback port.

```
CE1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
LC 5.5.5.5/32 is directly connected, 29:40:05, loopback0
O 8.8.8.8/32 [110/4] via 95.1.1.1, 00:00:02, vlan2
O 90.1.0.0/16 [110/3] via 95.1.1.1, 00:00:02, vlan2
C 95.1.0.0/16 is directly connected, 04:22:46, vlan2
L 95.1.1.2/32 is directly connected, 04:22:46, vlan2
C 98.1.0.0/16 is directly connected, 05:05:23, vlan3
L 98.1.1.1/32 is directly connected, 05:05:23, vlan3
C 127.0.0.0/8 is directly connected, 241:57:31, lo0
L 127.0.0.1/32 is directly connected, 241:57:31, lo0
```

```
CE1#traceroute 8.8.8.8
Type escape sequence to abort.
Tracing the route to 8.8.8.8 , min ttl = 1, max ttl = 30 .

 1 95.1.1.1  0 ms  0 ms  0 ms
 2 93.1.1.1 [MPLS: Labels 16/5120 Exp 0]  0 ms  0 ms  0 ms
 3 92.1.1.1 [MPLS: Labels 5120 Exp 0] 0 ms  0 ms  0 ms
 4 8.8.8.8  16 ms  0 ms  0 ms
```

It is indicated that the path from CE1 to CE2 passes through the bone global network.

### 79.3.7 Intranet access to the Internet

#### Network Requirements

- PE1 and PE2 are connected to the CE of VPN1, and CE1 and CE2 belong to the same VPN.

- The Internet gateway is the router outside the VPN, and all sites inside the VPN are connected to the Internet through the Intranet.
- VPN members forward their access to the Internet by importing a default route to access the Internet to the CE (CE1) that connects to the Internet gateway.
- Configure OSPF between PEs to achieve intra-PE communication, and configure MP-IBGP to exchange VPN routing information.

### Network Topology

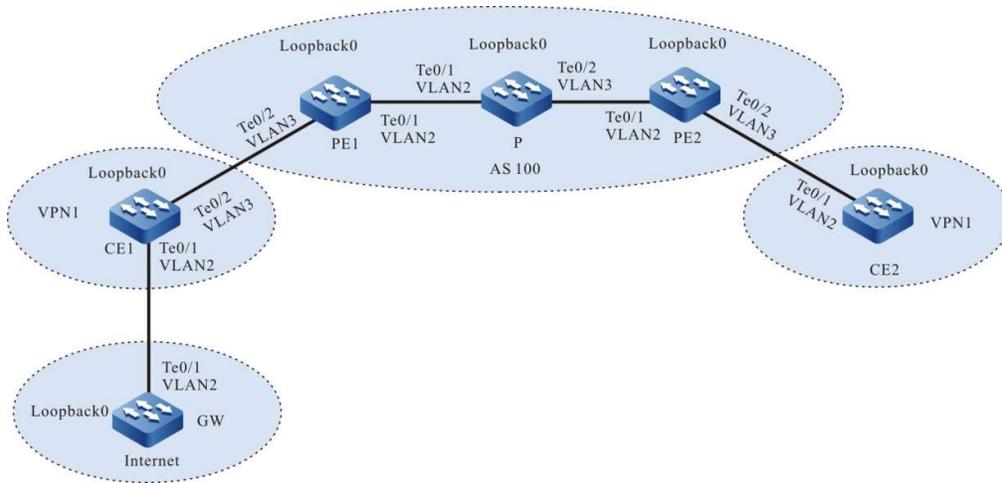


Figure 21-22 Network Topology of Intranet Access to the Internet

Table 79-45 Interface Mapping Relationships

of equipment	Interface	IP address	of equipment	Interface	IP address
CE1	Vlan3	95.1.1.2/16	P	Loopback0	11.11.11.11/32
	Vlan2	98.1.1.1/16	PE2	Vlan2	92.1.1.1/16
	Loopback0	5.5.5.5/32		Vlan3	90.1.1.1/16
PE1	Vlan2	93.1.1.2/16		Loopback0	75.75.75.75/32
	Vlan3	95.1.1.1/16	CE2	Vlan2	90.1.1.2/16
	Loopback0	90.90.90.90/32		Loopback0	8.8.8.8/32
P	Vlan2	93.1.1.1/16	GW	Vlan2	98.1.1.2/16
	Vlan3	92.1.1.2/16		Loopback0	1.1.1.1/32

## Configuration Steps

- Step 1: Configure the VLAN and add the port to the corresponding VLAN in access mode.  
(Omitted)
- Step 2: Configure IP addresses for the ports. (Omitted)
- Step 3: Configure global OSPF to advertise global routes.

#Configure global OSPF on PE1.

```
PE1#configure terminal
PE1(config)#router ospf 100
PE1(config-ospf)#network 90.90.90.0 0.0.0.0 area 0
PE1(config-ospf)#network 93.1.0.0 0.0.255.255 area 0
PE1(config-ospf)#exit
```

# Configure global OSPF on P.

```
P#configure terminal
P(config)#router ospf 100
P(config-ospf)#network 11.11.11.11 0.0.0.0 area 0
P(config-ospf)#network 92.1.0.0 0.0.255.255 area 0
P(config-ospf)#network 93.1.0.0 0.0.255.255 area 0
P(config-ospf)#exit
```

#Configure global OSPF on PE2.

```
PE2#configure terminal
PE2(config)#router ospf 100
PE2(config-ospf)#network 75.75.75.75 0.0.0.0 area 0
PE2(config-ospf)#network 92.1.0.0 0.0.255.255 area 0
PE2(config-ospf)#exit
```

#After the configuration is complete, view the global routing table on the device.

Take PE1 as an example:

```
PE1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

O 11.11.11.11/32 [110/2] via 93.1.1.1, 00:06:12, vlan2
O 75.75.75.75/32 [110/3] via 93.1.1.1, 00:06:03, vlan2
LC 90.90.90.90/32 is directly connected, 154:02:28, loopback0
```

```
C 93.1.0.0/16 is directly connected, 00:34:54, vlan2
L 93.1.1.2/32 is directly connected, 00:34:54, vlan2
O 92.1.0.0/16 [110/2] via 93.1.1.1, 00:08:12, vlan2
```

It is indicated that the routing information of PE2 and P's loopback port exists in the global routing table of PE1.

---

## Note

- Refer to PE1 for the inspection method of P and PE2.
- 

Step 4: Enable MPLS IP and MPLS LDP.

#Enable global MPLS IP and MPLS LDP on PE1, and also enable MPLS IP and MPLS LDP on the interface.

```
PE1(config)#mpls ip
PE1(config)#mpls ldp
PE1(config-ldp)#router-id 90.90.90.90
PE1(config-ldp)#address-family ipv4
PE1(config-ldp-af4)#transport-address 90.90.90.90
PE1(config-ldp-af4)#exit
PE1(config-ldp)#exit
PE1(config)#interface vlan2
PE1(config-if-vlan2)#mpls ip
PE1(config-if-vlan2)#mpls ldp
PE1(config-if-vlan2)#exit
```

# Enable global MPLS IP and MPLS LDP on P. Also enable MPLS IP and MPLS LDP on the interface.

```
P(config)#mpls ip
P(config)#mpls ldp
P(config-ldp)#router-id 11.11.11.11
P(config-ldp)#address-family ipv4
P(config-ldp-af4)#transport-address 11.11.11.11
P(config-ldp-af4)#exit
P(config-ldp)#exit
P(config)#interface vlan2
P(config-if-vlan2)#mpls ip
P(config-if-vlan2)#mpls ldp
P(config-if-vlan2)#exit
```

```
P(config)#interface vlan3
P(config-if-vlan3)#mpls ip
P(config-if-vlan3)#mpls ldp
P(config-if-vlan3)#exit
```

# Enable global MPLS IP and MPLS LDP on PE2, and also enable MPLS IP and MPLS LDP on the interface.

```
PE2(config)#mpls ip
PE2(config)#mpls ldp
PE2(config-ldp)#router-id 75.75.75.75
PE2(config-ldp)#address-family ipv4
PE2(config-ldp-af4)#transport-address 75.75.75.75
PE2(config-ldp-af4)#exit
PE2(config-ldp)#exit
PE2(config)#interface vlan2
PE2(config-if-vlan2)#mpls ip
PE2(config-if-vlan2)#mpls ldp
PE2(config-if-vlan2)#exit
```

# After the configuration is complete, view the LDP session information on the device.

Take PE1 as an example:

```
PE1#show mpls ldp session
Peer IP Address  Peer Type  My Role  State    DS Cap  DeadTime
11.11.11.11     Multicast  Active   OPERATIONAL  Disabled 00:02:20
Statistics for ldp sessions:
  Multicast sessions: 1
  Targeted sessions: 0
```

It is indicated that PE1 successfully establishes an LDP session with P.

#View the routing label table entries on the device.

Take PE1 as an example:

```
PE1#show ip route 11.11.11.11 detail
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

O 11.11.11.11/32 [110/2] via 93.1.1.1, label 3, 14:29:21, vlan2
                               93.1.1.1 [0], vlan2
```

```
PE1#show ip route 75.75.75.75 detail
```

```
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
```

```
U - Per-user Static route
```

```
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
O 75.75.75.75/32 [110/3] via 93.1.1.1, label 16, 14:30:21, vlan2  
93.1.1.1 [0], vlan2
```

It is indicated the label information of the loopback ports to P and PE2 exist on PE1.

---

## Note

- Refer to PE1 for the inspection method of P and PE2.
- 

Step 5: Configure the VPN instance to advertise the CE route to the PE via OSPF.

#Configure VPN instance and OSPF under VPN instance on PE1.

```
PE1(config)#ip vrf 1  
PE1(config-vrf)#rd 100:1  
PE1(config-vrf)#route-target export 100:1  
PE1(config-vrf)#route-target import 100:1  
PE1(config-vrf)#exit  
PE1(config)#interface vlan3  
PE1(config-if-vlan3)#ip vrf forwarding 1  
PE1(config-if-vlan3)#ip address 95.1.1.1 255.255.0.0  
PE1(config-if-vlan3)#exit  
PE1(config)#router ospf 200 vrf 1  
PE1(config-ospf)#network 95.1.0.0 0.0.255.255 area 0  
PE1(config-ospf)#exit
```

#Configure OSPF on CE1.

```
CE1#configure terminal  
CE1(config)#router ospf 100  
CE1(config-ospf)#network 5.5.5.5 0.0.0.0 area 0  
CE1(config-ospf)#network 95.1.0.0 0.0.255.255 area 0  
CE1(config-ospf)#exit
```

#Configure VPN instance and OSPF under VPN instance on PE2.

```
PE2(config)#ip vrf 1
PE2(config-vrf)#rd 100:1
PE2(config-vrf)#route-target export 100:1
PE2(config-vrf)#route-target import 100:1
PE2(config-vrf)#exit
PE2(config)#interface vlan3
PE2(config-if-vlan3)#ip vrf forwarding 1
PE2(config-if-vlan3)#ip address 90.1.1.1 255.255.0.0
PE2(config-if-vlan3)#exit
PE2(config)#router ospf 200 vrf 1
PE2(config-ospf)#network 90.1.0.0 0.0.255.255 area 0
PE2(config-ospf)#exit
```

#Configure OSPF on CE2.

```
CE2#configure terminal
CE2(config)#router ospf 100
CE2(config-ospf)#network 8.8.8.8 0.0.0.0 area 0
CE2(config-ospf)#network 90.1.0.0 0.0.255.255 area 0
CE2(config-ospf)#exit
```

#After the configuration is complete, view the VPN routing table on the PE.

Take PE1 as an example:

```
PE1#show ip route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

O 5.5.5.5/32 [110/2] via 95.1.1.2, 00:11:11, vlan3
C 95.1.0.0/16 is directly connected, 00:11:45, vlan3
L 95.1.1.1/32 is directly connected, 00:11:45, vlan3
```

It is indicated the loopback port routing information to CE1 exists in the VPN routing table of PE1.

---

## Note

- Refer to PE1 for the inspection method of PE2.

Step 6: Configure the MP-IBGP to use the loopback interface as the peer address; and redistribute routes with each other and the IGP protocol under the VPN instance.

#Configure the MP-IBGP on PE1 to enable VPNv4 address clustering; and redistribute routes with each other and the IGP protocol under the VPN instance.

```
PE1(config)#router bgp 100
PE1(config-bgp)#neighbor 75.75.75.75 remote-as 100
PE1(config-bgp)#neighbor 75.75.75.75 update-source loopback0
PE1(config-bgp)#address-family vpnv4
PE1(config-bgp-af)#neighbor 75.75.75.75 activate
PE1(config-bgp-af)#neighbor 75.75.75.75 send-community extended
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#address-family ipv4 vrf 1
PE1(config-bgp-af)#redistribute ospf 200
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
PE1(config)#router ospf 200 vrf 1
PE1(config-ospf)#redistribute bgp 100
PE1(config-ospf)#exit
```

#Configure the MP-IBGP on PE2 to enable VPNv4 address clustering; and redistribute routes with each other and the IGP protocol under the VPN instance.

```
PE2(config)#router bgp 100
PE2(config-bgp)#neighbor 90.90.90.90 remote-as 100
PE2(config-bgp)#neighbor 90.90.90.90 update-source loopback0
PE2(config-bgp)#address-family vpnv4
PE2(config-bgp-af)#neighbor 90.90.90.90 activate
PE2(config-bgp-af)#neighbor 90.90.90.90 send-community extended
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#address-family ipv4 vrf 1
PE2(config-bgp-af)#redistribute ospf 200
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#exit
PE2(config)#router ospf 200 vrf 1
PE2(config-ospf)#redistribute bgp 100
PE2(config-ospf)#exit
```

# After the configuration is complete, view the BGP neighbor information on the PE.

Take PE1 as an example:

```
PE1#show ip bgp vpnv4 all summary
```

BGP router identifier 90.90.90.90, local AS number 100

BGP table version is 6

1 BGP AS-PATH entries

0 BGP community entries

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
75.75.75.75	4	100	40	41	5	0	0	00:32:01	4

Total number of neighbors 1

The successful establishment of BGP neighbors between PE1 and PE2 can be seen from the fact that the contents of the column State/PfxRcd are shown as numbers (the number of received route prefixes from neighbors).

#View the BGP VPNv4 routing table and the routing table of VPN1 on the PE.

Take PE1 as an example:

```
PE1#show ip bgp vpnv4 vrf 1
```

BGP table version is 39, local router ID is 90.90.90.90

Status codes: s suppressed, d damped, h history, \* valid, > best, i - internal,

S Stale

Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
---------	----------	--------	--------	--------	------

Route Distinguisher: 100:1 (Default for VRF 1)

[O]*> 5.5.5.5/32	95.1.1.2	2			32768 ?
[B]*>i8.8.8.8/32	75.75.75.75	2	100		0 ?
[B]*>i90.1.0.0/16	75.75.75.75	1	100		0 ?
[O]*> 95.1.0.0/16	0.0.0.0	1			32768 ?

```
PE1#show ip route vrf 1
```

Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS

U - Per-user Static route

O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

O 5.5.5.5/32 [110/2] via 95.1.1.2, 00:50:39, vlan3

B 8.8.8.8/32 [200/2] via 75.75.75.75, 00:20:04, vlan2

B 90.1.0.0/16 [200/1] via 75.75.75.75, 00:20:04, vlan2

C 95.1.0.0/16 is directly connected, 00:51:28, vlan3

L 95.1.1.1/32 is directly connected, 00:51:28, vlan3

It is indicated that routing information to CE2 exists in both the BGP VPNv4 routing table of PE1 and the routing table of VPN1.

#View the routing label table entries and MPLS forwarding table on the PE.

Take PE1 as an example:

```
PE1#show ip route vrf 1 8.8.8.8 detail
```

```
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
```

```
U - Per-user Static route
```

```
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
B 8.8.8.8/32 [200/0] via 75.75.75.75, label 5120, 01:04:26, vlan2
    93.1.1.1 [3], label 16, vlan2
```

```
PE1#show mpls forwarding-table
```

```
Pro: L - LDP, B - MP-BGP, R - RSVP, M - Mapped-Route, ML - mLDP (ML FEC: Root
address/OT/OV), RM - RSVP P2MP (RM FEC: P2MP ID/TID)
```

```
S - Static Label
```

Pro	Ident	FEC	Inlabel	Outlabel	Outgoing	Next hop
B	1	0.0.0.0/0	5120	/	/	/

It is indicated that the route label information of VPN1 exists in the forwarding table of PE1.

---

## Note

- The inspection method on PE2 is the same as PE1.
- 

Step 7: Configure static routes to enable VPN members to access the Internet.

#Configure the default route to the Internet on CE1.

```
CE1(config)#ip route 0.0.0.0 0.0.0.0 98.1.1.2
```

#Configure the default route to the Internet on PE1, redistribute this default route to BGP, and thus advertise the route to the Internet to the peer PE and CE.

```
PE1(config)#ip route vrf 1 0.0.0.0 0.0.0.0 95.1.1.2
```

```
PE1(config)#router bgp 100
```

```

PE1(config-bgp)#address-family ipv4 vrf 1
PE1(config-bgp-af)#redistribute static
PE1(config-bgp-af)#default-information originate
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit

```

#Enable the default route introduction feature under OSPF in PE2 to receive routes coming from redistribution.

```

PE2(config)#router ospf 200
PE2(config-ospf)#default-information originate
PE2(config-ospf)#exit

```

#Configure the default route on the Internet gateway.

```

GW#configure terminal
GW(config)#ip route 0.0.0.0 0.0.0.0 98.1.1.1

```

---

## Caution

- For BGP to redistribute default routes, it requires the configuration of **default-information originate**.
- 

Step 8: Check the result.

#After the configuration is complete, view the BGP VPNv4 routing table and the routing table of VPN1 on the device.

Take PE1 as an example:

```

PE1#show ip bgp vpnv4 vrf 1
BGP table version is 39, local router ID is 90.90.90.90
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop        Metric LocPrf Weight Path
Route Distinguisher: 100:1 (Default for VRF 1)
[S]*> 0.0.0.0/0    95.1.1.2        0   32768 ?
[B]*>i8.8.8/32    75.75.75.75     2  100  0 ?
[O]*> 5.5.5/32    95.1.1.2        2   32768 ?
[B]*>i90.1.0.0/16 75.75.75.75     1  100  0 ?
[O]*> 95.1.0.0/16 0.0.0.0         1   32768 ?

```

```
PE1#show ip route vrf 1
```

```
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
```

```
U - Per-user Static route
```

```
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
S 0.0.0.0 [1/10] via 95.1.1.2, 01:12:43, vlan3
O 5.5.5.5/32 [110/2] via 95.1.1.2, 01:11:55, vlan3
B 8.8.8.8/32 [200/2] via 75.75.75.75, 00:41:19, vlan2
B 90.1.0.0/16 [200/1] via 75.75.75.75, 00:41:19, vlan2
C 95.1.0.0/16 is directly connected, 01:12:43, vlan3
L 95.1.1.1/32 is directly connected, 01:12:43, vlan3
```

It is indicated that CE1 cannot ping through the loopback port of CE2.

# Check the accessibility of the device to the Internet.

```
PE1#ping vrf 1 1.1.1.1
```

```
Press key (ctrl + shift + 6) interrupt it.
```

```
Sending 5, 76-byte ICMP Echos to 98.1.1.2 , timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100% (5/5). Round-trip min/avg/max = 0/0/0 ms.
```

```
PE2#ping vrf 1 1.1.1.1
```

```
Press key (ctrl + shift + 6) interrupt it.
```

```
Sending 5, 76-byte ICMP Echos to 98.1.1.2 , timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100% (5/5). Round-trip min/avg/max = 0/0/0 ms.
```

```
CE2#ping 1.1.1.1
```

```
Press key (ctrl + shift + 6) interrupt it.
```

```
Sending 5, 76-byte ICMP Echos to 98.1.1.2 , timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100% (5/5). Round-trip min/avg/max = 0/3/16 ms.
```

It is indicated that PE1, PE2 and CE2 can all ping through the loopback port of the Internet gateway.

### 79.3.8 Service provider network access to the Internet way

#### Network Requirements

- PE1 and PE2 are connected to the CE of VPN1, and CE1 and CE2 belong to the same VPN.
- The Internet gateway is the router outside the VPN, and all sites inside the VPN are connected to the Internet through the service provider network.
- VPN members forward their access to the Internet by importing a default route to access the Internet to the PE (PE1) that connects to the Internet gateway.
- Configure OSPF between PEs to achieve intra-PE communication, and configure MP-IBGP to exchange VPN routing information.

#### Network Topology

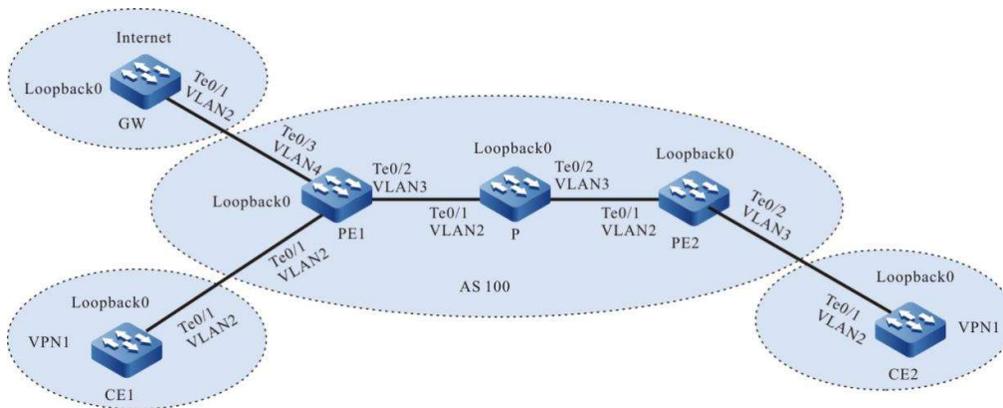


Figure 79-23 Network Topology of Ways of Service Provider Network Access to the Internet

Table 46-47 Interface Mapping Relationships

of equipment	Interface	IP address	of equipment	Interface	IP address
CE1	Vlan2	10.1.1.1/24	P	Loopback0	22.22.22.22/32
	Loopback0	1.1.1.1/32	PE2	Vlan2	10.1.3.2/24
PE1	Vlan2	10.1.1.2/24		Vlan3	10.1.4.1/24
	Vlan3	10.1.2.1/24		Loopback0	33.33.33.33/32
	Vlan4	10.1.5.1/24	CE2	Vlan2	10.1.4.2/24

of equipment	Interface	IP address	of equipment	Interface	IP address
	Loopback0	11.11.11.11/32		Loopback0	2.2.2.2/32
P	Vlan2	10.1.2.2/24	GW	Vlan2	10.1.5.2/24
	Vlan3	10.1.3.1/24		Loopback0	3.3.3.3/32

### Configuration Steps

Step 1: Configure the VLAN and add the port to the corresponding VLAN in access mode.  
(Omitted)

Step 2: Configure IP addresses for the ports. (Omitted)

Step 3: Configure global OSPF to advertise global routes.

#Configure global OSPF on PE1.

```
PE1#configure terminal
PE1(config)#router ospf 100
PE1(config-ospf)#network 10.1.2.0 0.0.0.255 area 0
PE1(config-ospf)#network 11.11.11.11 0.0.0.0 area 0
PE1(config-ospf)#exit
```

# Configure global OSPF on P.

```
P#configure terminal
P(config)#router ospf 100
P(config-ospf)#network 10.1.2.0 0.0.0.255 area 0
P(config-ospf)#network 10.1.3.0 0.0.0.255 area 0
P(config-ospf)#network 22.22.22.22 0.0.0.0 area 0
P(config-ospf)#exit
```

#Configure global OSPF on PE2.

```
PE2#configure terminal
PE2(config)#router ospf 100
PE2(config-ospf)#network 10.1.3.0 0.0.0.255 area 0
PE2(config-ospf)#network 33.33.33.33 0.0.0.0 area 0
PE2(config-ospf)#exit
```

#After the configuration is complete, view the global routing table on the device.

Take PE1 as an example:

```
PE1#show ip route
```

Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS

U - Per-user Static route

O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

```
C 10.1.2.0/24 is directly connected, 65:47:37, vlan3
L 10.1.2.1/32 is directly connected, 65:47:37, vlan3
O 10.1.3.0/24 [110/2] via 10.1.2.2, 01:18:39, vlan3
C 10.1.5.0/24 is directly connected, 00:22:25, vlan4
L 10.1.5.1/32 is directly connected, 00:22:25, vlan4
LC 11.11.11.11/32 is directly connected, 65:47:37, loopback0
O 22.22.22.22/32 [110/2] via 10.1.2.2, 65:11:53, vlan3
O 33.33.33.33/32 [110/3] via 10.1.2.2, 01:18:34, vlan3
C 127.0.0.0/8 is directly connected, 65:47:57, lo0
L 127.0.0.1/32 is directly connected, 65:47:57, lo0
```

It is indicated that the routing information of PE2 and P's loopback port exists in the global routing table of PE1.

---

## Note

- Refer to PE1 for the inspection method of P and PE2.
- 

Step 4: Enable MPLS IP and MPLS LDP.

#Enable global MPLS IP and MPLS LDP on PE1, and also enable MPLS IP and MPLS LDP on the interface.

```
PE1(config)#mpls ip
PE1(config)#mpls ldp
PE1(config-ldp)#router-id 11.11.11.11
PE1(config-ldp)#address-family ipv4
PE1(config-ldp-af4)#transport-address 11.11.11.11
PE1(config-ldp-af4)#exit
PE1(config-ldp)#exit
PE1(config)#interface vlan3
PE1(config-if-vlan3)#mpls ip
PE1(config-if-vlan3)#mpls ldp
```

```
PE1(config-if-vlan3)#exit
```

# Enable global MPLS IP and MPLS LDP on P. Also enable MPLS IP and MPLS LDP on the interface.

```
P(config)#mpls ip
P(config)#mpls ldp
P(config-ldp)#router-id 22.22.22.22
P(config-ldp)#address-family ipv4
P(config-ldp-af4)#transport-address 22.22.22.22
P(config-ldp-af4)#exit
P(config-ldp)#exit
P(config)#interface vlan2
P(config-if-vlan2)#mpls ip
P(config-if-vlan2)#mpls ldp
P(config-if-vlan2)#exit
P(config)#interface vlan3
P(config-if-vlan3)#mpls ip
P(config-if-vlan3)#mpls ldp
P(config-if-vlan3)#exit
```

# Enable global MPLS IP and MPLS LDP on PE2, and also enable MPLS IP and MPLS LDP on the interface.

```
PE2(config)#mpls ip
PE2(config)#mpls ldp
PE2(config-ldp)#router-id 33.33.33.33
PE2(config-ldp)#address-family ipv4
PE2(config-ldp-af4)#transport-address 33.33.33.33
PE2(config-ldp-af4)#exit
PE2(config-ldp)#exit
PE2(config)#interface vlan2
PE2(config-if-vlan2)#mpls ip
PE2(config-if-vlan2)#mpls ldp
PE2(config-if-vlan2)#exit
```

# After the configuration is complete, view the LDP session information on the device.

Take PE1 as an example:

```
PE1#show mpls ldp session
Peer IP Address Peer Type My Role State DS Cap DeadTime
22.22.22.22 Multicast Passive OPERATIONAL Disabled 00:02:34
Statistics for ldp sessions:
Multicast sessions: 1
Targeted sessions: 0
```

It is indicated that PE1 successfully establishes an LDP session with P.

#View the routing label table entries on the device.

Take PE1 as an example:

```
PE1#show ip route 22.22.22.22 detail
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
O 22.22.22.22/32 [110/2] via 10.1.2.2, label 3, 14:29:21, vlan3
    10.1.2.2 [0], vlan3
```

```
PE1#show ip route 33.33.33.33 detail
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
O 33.33.33.33/32 [110/3] via 10.1.2.2, label 17, 14:30:21, vlan3
    10.1.2.2 [0], vlan3
```

It is indicated the label information of the loopback ports to P and PE2 exist on PE1.

---

## Note

- Refer to PE1 equipment for the inspection method of P and PE2.
- 

Step 5: Configure the VPN instance to advertise the CE route to the PE via OSPF.

#Configure VPN instance and OSPF under VPN instance on PE1.

```
PE1(config)#ip vrf 1
PE1(config-vrf)#rd 100:1
PE1(config-vrf)#route-target export 100:1
PE1(config-vrf)#route-target import 100:1
```

```
PE1(config-vrf)#exit
PE1(config)#interface vlan2
PE1(config-if-vlan2)#ip vrf forwarding 1
PE1(config-if-vlan2)#ip address 10.1.1.2 255.255.255.0
PE1(config-if-vlan2)#exit
PE1(config)#router ospf 200 vrf 1
PE1(config-ospf)#network 10.1.1.0 0.255.255.255 area 0
PE1(config-ospf)#exit
```

#### #Configure OSPF on CE1.

```
CE1#configure terminal
CE1(config)#router ospf 100
CE1(config-ospf)#network 1.1.1.1 0.0.0.0 area 0
CE1(config-ospf)#network 10.1.1.0 0.0.0.255 area 0
CE1(config-ospf)#exit
```

#### #Configure VPN instance and OSPF under VPN instance on PE2.

```
PE2(config)#ip vrf 1
PE2(config-vrf)#rd 100:1
PE2(config-vrf)#route-target export 100:1
PE2(config-vrf)#route-target import 100:1
PE2(config-vrf)#exit
PE2(config)#interface vlan3
PE2(config-if-vlan3)#ip vrf forwarding 1
PE2(config-if-vlan3)#ip address 10.1.4.1 255.255.255.0
PE2(config)#exit
PE2(config)#router ospf 200 vrf 1
PE2(config-ospf)#network 10.1.4.0 0.0.0.255 area 0
PE2(config-ospf)#exit
```

#### #Configure OSPF on CE2.

```
CE2#configure terminal
CE2(config)#router ospf 100
CE2(config-ospf)#network 2.2.2.2 0.0.0.0 area 0
CE2(config-ospf)#network 10.1.4.0 0.0.0.255 area 0
CE2(config-ospf)#exit
```

#After the configuration is complete, view the VPN routing table on the PE.

Take PE1 as an example:

```
PE1#show ip route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
```

```
O 1.1.1.1/32 [110/2] via 10.1.1.1, 00:00:12, vlan2
C 10.1.1.0/24 is directly connected, 00:00:23, vlan2
L 10.1.1.2/32 is directly connected, 00:00:23, vlan2
```

It is indicated the loopback port routing information to CE1 exists in the VPN routing table of PE1.

---

## Note

- Refer to PE1 for the inspection method of PE2.
- 

Step 6: Configure the MP-IBGP to use the loopback interface as the peer address; and redistribute routes with each other and the IGP protocol under the VPN instance.

#Configure the MP-IBGP on PE1 to enable VPNv4 address clustering; and redistribute routes with each other and the IGP protocol under the VPN instance.

```
PE1(config)#router bgp 100
PE1(config-bgp)#neighbor 33.33.33.33 remote-as 100
PE1(config-bgp)#neighbor 33.33.33.33 update-source loopback0
PE1(config-bgp)#address-family vpnv4
PE1(config-bgp-af)#neighbor 33.33.33.33 activate
PE1(config-bgp-af)#neighbor 33.33.33.33 send-community extended
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#address-family ipv4 vrf 1
PE1(config-bgp-af)#redistribute ospf 200
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
PE1(config)#router ospf 200 vrf 1
PE1(config-ospf)#redistribute bgp 100
PE1(config-ospf)#exit
```

#Configure the MP-IBGP on PE2 to enable VPNv4 address clustering; and redistribute routes with each other and the IGP protocol under the VPN instance.

```
PE2(config)#router bgp 100
PE2(config-bgp)#neighbor 11.11.11.11 remote-as 100
```

```

PE2(config-bgp)#neighbor 11.11.11.11 update-source loopback0
PE2(config-bgp)#address-family vpnv4
PE2(config-bgp-af)#neighbor 11.11.11.11 activate
PE2(config-bgp-af)#neighbor 11.11.11.11 send-community extended
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#address-family ipv4 vrf 1
PE2(config-bgp-af)#redistribute ospf 200
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#exit
PE2(config)#router ospf 200 vrf 1
PE2(config-ospf)#redistribute bgp 100
PE2(config-ospf)#exit

```

# After the configuration is complete, view the BGP neighbor information on the PE.

Take PE1 as an example:

```

PE1#show ip bgp vpnv4 all summary
BGP router identifier 11.11.11.11, local AS number 100
BGP table version is 3
1 BGP AS-PATH entries
0 BGP community entries

Neighbor      V  AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down State/PfxRcd
33.33.33.33   4 100    8    9    3    0  00:04:26   2

Total number of neighbors 1

```

The successful establishment of BGP neighbors between PE1 and PE2 can be seen from the fact that the contents of the column State/PfxRcd are shown as numbers (the number of received route prefixes from neighbors).

#View the BGP VPNv4 routing table and the routing table of VPN1 on the PE.

Take PE1 as an example:

```

PE1#show ip bgp vpnv4 vrf 1
BGP table version is 3, local router ID is 11.11.11.11
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
                S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Network        Next Hop        Metric LocPrf Weight Path
Route Distinguisher: 100:1 (Default for VRF 1)
[O]*> 1.1.1.1/32  10.1.1.1        2    32768 ?
[B]*>i2.2.2.2/32  33.33.33.33     2 100  0 ?

```

```
[O]*> 10.1.1.0/24 0.0.0.0 1 32768 ?
[B]*>i10.1.4.0/24 33.33.33.33 1 100 0 ?
```

```
PE1#show ip route vrf 1
```

```
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
```

```
U - Per-user Static route
```

```
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
O 1.1.1.1/32 [110/2] via 10.1.1.1, 00:20:31, vlan2
B 2.2.2.2/32 [200/2] via 33.33.33.33, 00:08:17, vlan3
C 10.1.1.0/24 is directly connected, 00:20:42, vlan2
L 10.1.1.2/32 is directly connected, 00:20:42, vlan2
B 10.1.4.0/24 [200/1] via 33.33.33.33, 00:09:33, vlan3
```

It is indicated that routing information to CE2 exists in both the BGP VPNv4 routing table of PE1 and the routing table of VPN1.

#View the routing label table entries and MPLS forwarding table on the PE.

```
PE1#show ip route vrf 1 2.2.2.2 detail
```

```
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
```

```
U - Per-user Static route
```

```
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
B 2.2.2.2/32 [200/0] via 33.33.33.33, label 16, 01:04:26, vlan3
    10.1.2.2 [3], label 17, vlan3
```

```
PE1#show ip route vrf 1 10.1.4.0 detail
```

```
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
```

```
U - Per-user Static route
```

```
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
B 10.1.4.0/24 [200/0] via 33.33.33.33, label 16, 01:04:26, vlan3
    10.1.2.2 [3], label 17, vlan3
```

```
PE1#show mpls forwarding-table
```

```
Pro: L - LDP, B - MP-BGP, R - RSVP, M - Mapped-Route, ML - mLDP (ML FEC: Root  
address/OT/OV), RM - RSVP P2MP (RM FEC: P2MP ID/TID)
```

```
S - Static Label
```

Pro Ident	FEC	Inlabel	Outlabel	Outgoing	Next hop
B 1	0.0.0.0/0	16 / /	/	/	/

It is indicated that the route label information of VPN1 exists in the forwarding table of PE.

---

## Note

- The inspection method on PE2 is the same as PE1.
- 

Step 7: Configure static routes on PEs and CEs to enable VPN members to access the Internet.

#Configure the default route to the Internet on CE1.

```
CE1(config)#ip route 0.0.0.0 0.0.0.0 10.1.1.2
```

#Configure the default route to the Internet and the route to CE1 globally on PE1, configure the default route to the Internet across VPNs under VPN, and cancel configuration of sole assignment and reception of labels for 32-bit mask within the MPLS LDP process.

```
PE1(config)#ip route 0.0.0.0 0.0.0.0 10.1.5.2  
PE1(config)#ip route vrf global 1.1.1.1 255.255.255.255 10.1.1.1 vrf 1  
PE1(config)#ip route vrf global 10.1.1.0 255.255.255.0 10.1.1.1 vrf 1  
PE1(config)#ip route vrf 1 0.0.0.0 0.0.0.0 10.1.5.2 vrf global  
PE1(config)#router bgp 100  
PE1(config-bgp)#address-family ipv4 vrf 1  
PE1(config-bgp-af)#redistribute connected  
PE1(config-bgp-af)#exit-address-family  
PE1(config-bgp)#exit  
PE1(config)#mpls ldp  
PE1(config-ldp)#address-family ipv4  
PE1(config-ldp-af4)#no advertise-labels for 32bit-mask-fec-only  
PE1(config-ldp-af4)#no accept-labels for 32bit-mask-fec-only  
PE1(config-ldp-af4)#exit  
PE1(config-ldp)#exit
```

#Configure the route to CE2 globally on PE2, configure the cross-VPN default route to the Internet under VPN with the next hop as PE2's BGP neighbor address, and redistribute the global static route under global OSPF to redistribute the route to the private network to PE1, and remove the 32-bit mask assignment and receive labels only under the MPLS LDP process.

```
PE2(config)#ip route vrf global 2.2.2.2 255.255.255.255 10.1.4.2 vrf 1
PE2(config)#ip route vrf global 10.1.4.0 255.255.255.0 10.1.4.2 vrf 1
PE2(config)#ip route vrf 1 0.0.0.0 0.0.0.0 11.11.11.11 vrf global
PE2(config)#router ospf 100
PE2(config-ospf)#redistribute static
PE2(config-ospf)#exit
PE2(config)#mpls ldp
PE2(config-ldp)#address-family ipv4
PE2(config-ldp-af4)#no advertise-labels for 32bit-mask-fec-only
PE2(config-ldp-af4)#no accept-labels for 32bit-mask-fec-only
PE2(config-ldp-af4)#exit
PE2(config-ldp)#exit
```

#Configure on CE2 the default route to the Internet.

```
CE2(config)#ip route 0.0.0.0 0.0.0.0 10.1.4.1
```

#Configure the default route on the Internet gateway.

```
GW#configure terminal
GW(config)#ip route 0.0.0.0 0.0.0.0 10.1.5.1
```

Step 8: Check the result.

#After the configuration is complete, view the global routing table on the PE.

Take PE1 as an example:

```
PE1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

S 0.0.0/0 [1/10] via 10.1.5.2, 00:11:42, vlan4
S 1.1.1/32 [1/10] via 10.1.1.1, 95:27:42, vlan2
OE 2.2.2/32 [150/20] via 10.1.2.2, 00:13:22, vlan3
S 10.1.1.0/24 [1/10] via 10.1.1.1, 95:27:49, vlan2
C 10.1.2.0/24 is directly connected, 96:57:55, vlan3
L 10.1.2.1/32 is directly connected, 96:57:55, vlan3
O 10.1.3.0/24 [110/2] via 10.1.2.2, 72:44:34, vlan3
```

```
OE 10.1.4.0/24 [150/20] via 10.1.2.2, 00:13:22, vlan3
C 10.1.5.0/24 is directly connected, 96:57:41, vlan4
L 10.1.5.1/32 is directly connected, 96:57:41, vlan4
LC 11.11.11.11/32 is directly connected, 96:47:46, loopback0
O 22.22.22.22/32 [110/2] via 10.1.2.2, 72:44:34, vlan3
O 33.33.33.33/32 [110/3] via 10.1.2.2, 00:14:28, vlan3
C 127.0.0.0/8 is directly connected, 458:41:50, lo0
L 127.0.0.1/32 is directly connected, 458:41:50, lo0
```

```
PE1#show ip route vrf 1
```

```
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
```

```
U - Per-user Static route
```

```
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
S 0.0.0.0 [1/10] via 10.1.5.2, 95:27:24, vlan4
O 1.1.1.1/32 [110/2] via 10.1.1.1, 95:57:17, vlan2
B 2.2.2.2/32 [200/2] via 33.33.33.33, 00:13:44, vlan3
C 10.1.1.0/24 is directly connected, 95:57:28, vlan2
L 10.1.1.2/32 is directly connected, 95:57:28, vlan2
B 10.1.4.0/24 [200/0] via 33.33.33.33, 00:14:12, vlan3
```

It is indicated that both the global routing table and the VPN routing table on PE1 have a default route pointing to the Internet.

---

## Note

- Refer to PE1 device for the inspection method of PE2.
- 

# View the device's reachability to the Internet.

```
CE1#ping 3.3.3.3
```

```
Press key (ctrl + shift + 6) interrupt it.
```

```
Sending 5, 76-byte ICMP Echos to 3.3.3.3 , timeout is 2 seconds:
```

```
!!!!
```



Figure 24-25 Network Topology for Configuring a Shared VPN

Table 48-49 Interface Mapping Relationships

of equipment	Interface	IP address	of equipment	Interface	IP address
CE1	Vlan2	10.1.1.1/24	PE2	Vlan3	10.1.4.1/24
	Loopback0	1.1.1.1/32		Loopback0	22.22.22.22/32
PE1	Vlan2	10.1.1.2/24	PE3	Vlan2	10.1.2.2/24
	Vlan3	10.1.2.1/24		Vlan3	10.1.4.2/24
	Loopback0	11.11.11.11/32		Vlan4	10.1.3.1/24
CE2	Vlan2	10.1.5.1/24		Loopback0	33.33.33.33/32
	Loopback0	2.2.2.2/32	CE3	Vlan2	10.1.3.2/24
PE2	Vlan2	10.1.5.2/24		Loopback0	3.3.3.3/32

### Configuration Steps

- Step 1: Configure the VLAN and add the port to the corresponding VLAN in access mode. (Omitted)
- Step 2: Configure IP addresses for the ports. (Omitted)
- Step 3: Configure global OSPF to advertise global routes.

#Configure global OSPF on PE1.

```
PE1#configure terminal
PE1(config)#router ospf 100
PE1(config-ospf)#network 10.1.2.0 0.0.0.255 area 0
PE1(config-ospf)#network 11.11.11.11 0.0.0.0 area 0
PE1(config-ospf)#exit
```

#Configure global OSPF on PE2.

```
PE2#configure terminal
PE2(config)#router ospf 100
PE2(config-ospf)#network 10.1.4.0 0.0.0.255 area 0
PE2(config-ospf)#network 22.22.22.22 0.0.0.0 area 0
PE2(config-ospf)#exit
```

#Configure global OSPF on PE3.

```
PE3#configure terminal
PE3(config)#router ospf 100
PE3(config-ospf)#network 10.1.2.0 0.0.0.255 area 0
PE3(config-ospf)#network 10.1.4.0 0.0.0.255 area 0
PE3(config-ospf)#network 33.33.33.33 0.0.0.0 area 0
PE3(config-ospf)#exit
```

#After the configuration is complete, view the global routing table on the device.

Take PE1 as an example:

```
PE1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
C 10.1.2.0/24 is directly connected, 04:39:17, vlan3
L 10.1.2.1/32 is directly connected, 04:39:17, vlan3
O 10.1.4.0/24 [110/2] via 10.1.2.2, 03:46:04, vlan3
LC 11.11.11.11/32 is directly connected, 04:39:05, loopback0
O 22.22.22.22/32 [110/3] via 10.1.2.2, 03:46:04, vlan3
O 33.33.33.33/32 [110/2] via 10.1.2.2, 03:45:25, vlan3
C 127.0.0.0/8 is directly connected, 1579:41:11, lo0
L 127.0.0.1/32 is directly connected, 1579:41:11, lo0
```

It is indicated that the routing information of the loopback ports of PE2 and PE3 exists in the global routing table of PE1.

---

## Note

- Refer to PE1 for the inspection method of PE3 and PE2.
- 

Step 4: Enable MPLS IP and MPLS LDP.

#Enable global MPLS IP and MPLS LDP on PE1, and also enable MPLS IP and MPLS LDP on the interface.

```
PE1(config)#mpls ip
```

```
PE1(config)#mpls ldp
PE1(config-ldp)#router-id 11.11.11.11
PE1(config-ldp)#address-family ipv4
PE1(config-ldp-af4)#transport-address 11.11.11.11
PE1(config-ldp-af4)#exit
PE1(config-ldp)#exit
PE1(config)#interface vlan3
PE1(config-if-vlan3)#mpls ip
PE1(config-if-vlan3)#mpls ldp
PE1(config-if-vlan3)#exit
```

# Enable global MPLS IP and MPLS LDP on PE2, and also enable MPLS IP and MPLS LDP on the interface.

```
PE2(config)#mpls ip
PE2(config)#mpls ldp
PE2(config-ldp)#router-id 22.22.22.22
PE2(config-ldp)#address-family ipv4
PE2(config-ldp-af4)#transport-address 22.22.22.22
PE2(config-ldp-af4)#exit
PE2(config-ldp)#exit
PE2(config)#interface vlan3
PE2(config-if-vlan3)#mpls ip
PE2(config-if-vlan3)#mpls ldp
PE2(config-if-vlan3)#exit
```

# Enable global MPLS IP and MPLS LDP on PE3, and also enable MPLS IP and MPLS LDP on the interface.

```
PE3(config)#mpls ip
PE3(config)#mpls ldp
PE3(config-ldp)#router-id 33.33.33.33
PE3(config-ldp)#address-family ipv4
PE3(config-ldp-af4)#transport-address 33.33.33.33
PE3(config-ldp-af4)#exit
PE3(config-ldp)#exit
PE3(config)#interface vlan2
PE3(config-if-vlan2)#mpls ip
PE3(config-if-vlan2)#mpls ldp
PE3(config-if-vlan2)#exit
PE3(config)#interface vlan3
PE3(config-if-vlan3)#mpls ip
PE3(config-if-vlan3)#mpls ldp
PE3(config-if-vlan3)#exit
```

# After the configuration is complete, view the LDP session information on the device.

Take PE1 as an example:

```
PE1#show mpls ldp session
Peer IP Address Peer Type My Role State DS Cap DeadTime
33.33.33.33 Multicast Passive OPERATIONAL Disabled 00:02:48
Statistics for ldp sessions:
Multicast sessions: 1
Targeted sessions: 0
```

It is indicated that PE1 and PE3 successfully establish the LDP session.

#View the MPLS forwarding table on the device.

Take PE1 as an example:

```
PE1#show ip route 22.22.22.22 detail
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
U - Per-user Static route
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
O 22.22.22.22/32 [110/3] via 10.1.2.2, label 17, 14:29:21, vlan3
10.1.2.2 [0], vlan3
```

```
PE1#show ip route 33.33.33.33 detail
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
U - Per-user Static route
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
O 33.33.33.33/32 [110/2] via 10.1.2.2, label 3, 14:30:21, vlan3
10.1.2.2 [0], vlan3
```

It is indicated the label information of the loopback ports to PE2 and PE3 exist on PE1.

---

## Note

- Refer to PE1 for the inspection method of PE2 and PE3.
-

Step 5: Configure the VPN instance to advertise the CE route to the PE via OSPF.

#Configure VPN instance and OSPF under VPN instance on PE1.

```
PE1(config)#ip vrf 1
PE1(config-vrf)#rd 100:1
PE1(config-vrf)#route-target export 100:1
PE1(config-vrf)#route-target import 100:1
PE1(config-vrf)#route-target export 1100:1
PE1(config-vrf)#route-target import 1000:1
PE1(config-vrf)#exit
PE1(config)#interface vlan2
PE1(config-if-vlan2)#ip vrf forwarding 1
PE1(config-if-vlan2)#ip address 10.1.1.2 255.255.255.0
PE1(config-if-vlan2)#exit
PE1(config)#router ospf 200 vrf 1
PE1(config-ospf)#network 10.1.1.0 0.0.0.255 area 0
PE1(config-ospf)#exit
```

---

### Note

- The import-target and export-target of 100:1 in the Rt attribute of PE1 are for importing and exporting internal VPN routes, the export-target of 1100:1 is for exporting internal VPN routes to the shared VPN, and the import-target of 1000:1 is for importing routes passed by the shared VPN.
- 

#Configure OSPF on CE1.

```
CE1#configure terminal
CE1(config)#router ospf 100
CE1(config-ospf)#network 1.1.1.1 0.0.0.0 area 0
CE1(config-ospf)#network 10.1.1.0 0.0.0.255 area 0
CE1(config-ospf)#exit
```

#Configure VPN instance and OSPF under VPN instance on PE2.

```
PE2(config)#ip vrf 1
PE2(config-vrf)#rd 200:1
PE2(config-vrf)#route-target export 200:1
PE2(config-vrf)#route-target import 200:1
```

```
PE2(config-vrf)#route-target export 1100:1
PE2(config-vrf)#route-target import 1000:1
PE2(config-vrf)#exit
PE2(config)#interface vlan2
PE2(config-if-vlan2)#ip vrf forwarding 1
PE2(config-if-vlan2)#ip address 10.1.5.2 255.255.255.0
PE2(config-if-vlan2)#exit
PE2(config)#router ospf 200 vrf 1
PE2(config-ospf)#network 10.1.5.0 0.0.0.255 area 0
PE2(config-ospf)#exit
```

---

## Note

- The import-target and export-target of 200:1 in the Rt attribute of PE2 are for importing and exporting internal VPN routes, the export-target of 1100:1 is for exporting internal VPN routes to the shared VPN, and the import-target of 1000:1 is for importing routes passed by the shared VPN.
- 

### #Configure OSPF on CE2.

```
CE2#configure terminal
CE2(config)#router ospf 100
CE2(config-ospf)#network 2.2.2.2 0.0.0.0 area 0
CE2(config-ospf)#network 10.1.5.0 0.0.0.255 area 0
CE2(config-ospf)#exit
```

### #Configure VPN instance and OSPF under VPN instance on PE3.

```
PE3(config)#ip vrf vpn-share
PE3(config-vrf)#rd 300:1
PE3(config-vrf)#route-target export 1000:1
PE3(config-vrf)#route-target import 1100:1
PE3(config-vrf)#exit
PE3(config)#interface vlan4
PE3(config-if-vlan4)#ip vrf forwarding vpn-share
PE3(config-if-vlan4)#ip address 10.1.3.1 255.255.255.0
PE3(config-if-vlan4)#exit
PE3(config)#router ospf 200 vrf vpn-share
PE3(config-ospf)#network 10.1.3.0 0.0.0.255 area 0
PE3(config-ospf)#exit
```

---

## Note

- The export-target of 1000:1 in the Rt attribute of PE3 is used to export routes from the local VPN to other VPNs, and the import-target of 1100:1 is used to import routes coming from other VPNs.
- 

#Configure OSPF on CE3.

```
CE2#configure terminal
CE2(config)#router ospf 100
CE2(config-ospf)#network 3.3.3.3 0.0.0.0 area 0
CE2(config-ospf)#network 10.1.3.0 0.0.0.255 area 0
CE2(config-ospf)#exit
```

#After the configuration is complete, view the VPN routing table on the PE.

Take PE1 as an example:

```
PE1#show ip route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

O 1.1.1.1/32 [110/2] via 10.1.1.1, 04:09:32, vlan2
C 10.1.1.0/24 is directly connected, 04:19:47, vlan2
L 10.1.1.2/32 is directly connected, 04:19:47, vlan2
```

It is indicated the loopback port routing information to CE1 exists in the VPN routing table of PE1.

---

## Note

- Refer to PE1 for the inspection method of PE2 and PE3.
- 

Step 6: Configure the MP-IBGP to use the loopback interface as the peer address; and redistribute routes with each other and the IGP protocol under the VPN instance.

#Configure the MP-IBGP on PE1 to establish BGP neighbors with PE3, enable VPNv4 address clustering; and redistribute routes with each other and the IGP protocol under the VPN instance.

```
PE1(config)#router bgp 100
PE1(config-bgp)#neighbor 33.33.33.33 remote-as 100
PE1(config-bgp)#neighbor 33.33.33.33 update-source loopback0
PE1(config-bgp)#address-family vpnv4
PE1(config-bgp-af)#neighbor 33.33.33.33 activate
PE1(config-bgp-af)#neighbor 33.33.33.33 send-community extended
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#address-family ipv4 vrf 1
PE1(config-bgp-af)#redistribute ospf 200
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
PE1(config)#router ospf 200 vrf 1
PE1(config-ospf)#redistribute bgp 100
PE1(config-ospf)#exit
```

#Configure the MP-IBGP on PE2, establish BGP neighbors with PE3, enable VPNv4 address clustering; and redistribute routes with each other and the IGP protocol under the VPN instance.

```
PE2(config)#router bgp 100
PE2(config-bgp)#neighbor 33.33.33.33 remote-as 100
PE2(config-bgp)#address-family vpnv4
PE2(config-bgp-af)#neighbor 33.33.33.33 activate
PE2(config-bgp-af)#neighbor 33.33.33.33 send-community extended
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#address-family ipv4 vrf 1
PE2(config-bgp-af)#redistribute ospf 200
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#exit
PE2(config)#router ospf 200 vrf 1
PE2(config-ospf)#redistribute bgp 100
PE2(config-ospf)#exit
```

#Configure the MP-IBGP on PE3, establish BGP neighbors with PE1 and PE2, and enable VPNv4 address clustering; and redistribute routes with each other and the IGP protocol under the VPN instance.

```
PE3(config)#router bgp 100
PE3(config-bgp)#neighbor 11.11.11.11 remote-as 100
PE3(config-bgp)#neighbor 11.11.11.11 update-source loopback0
PE3(config-bgp)#neighbor 22.22.22.22 remote-as 100
PE3(config-bgp)#neighbor 22.22.22.22 update-source loopback0
PE3(config-bgp)#address-family vpnv4
```

```

PE3(config-bgp-af)#neighbor 11.11.11.11 activate
PE3(config-bgp-af)#neighbor 11.11.11.11 send-community extended
PE3(config-bgp-af)#neighbor 22.22.22.22 activate
PE3(config-bgp-af)#neighbor 22.22.22.22 send-community extended
PE3(config-bgp-af)#exit-address-family
PE3(config-bgp)#address-family ipv4 vrf vpn-share
PE3(config-bgp-af)#redistribute ospf 200
PE3(config-bgp-af)#exit-address-family
PE3(config-bgp)#exit
PE3(config)#router ospf 200 vrf vpn-share
PE3(config-ospf)#redistribute bgp 100
PE3(config-ospf)#exit

```

Step 7: Check the result.

# View BGP neighbor information on the PE.

Take PE1 as an example:

```

PE1#show ip bgp vpnv4 all summary
BGP router identifier 11.11.11.11, local AS number 100
BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries

Neighbor      V  AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down State/PfxRcd
33.33.33.33   4  100   305   302    2   0  0 04:16:40    2

Total number of neighbors 1

```

The successful establishment of BGP neighbors between PE1 and PE3 can be seen from the fact that the contents of the column State/PfxRcd are shown as numbers (the number of received route prefixes from neighbors).

#View the BGP VPNv4 routing table and the routing table of VPN1 on the PE.

Take PE1 as an example:

```

PE1#show ip bgp vpnv4 vrf 1
BGP table version is 2, local router ID is 11.11.11.11
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
                S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Network      Next Hop      Metric LocPrf Weight Path
Route Distinguisher: 100:1 (Default for VRF 1)

```

```
[O]*> 1.1.1.1/32    10.1.1.1        2    32768 ?
[B]*>i3.3.3.3/32    33.33.33.33     2    100   0 ?
[O]*> 10.1.1.0/24   0.0.0.0         1    32768 ?
[B]*>i10.1.3.0/24   33.33.33.33     1    100   0 ?
```

```
PE1#show ip route vrf 1
```

```
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
```

```
U - Per-user Static route
```

```
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
O 1.1.1.1/32 [110/2] via 10.1.1.1, 04:48:39, vlan2
B 3.3.3.3/32 [200/2] via 33.33.33.33, 04:46:00, vlan3
C 10.1.1.0/24 is directly connected, 04:58:53, vlan2
L 10.1.1.2/32 is directly connected, 04:58:53, vlan2
B 10.1.3.0/24 [200/1] via 33.33.33.33, 04:46:00, vlan3
```

It is indicated that there is routing information to CE3 in both the BGP VPNv4 routing table of PE1 and the routing table of VPN1, and there is no routing information to CE2.

#View the routing label table entries and MPLS forwarding table on the PE.

Take PE1 as an example:

```
PE1#show ip route vrf 1 3.3.3.3 detail
```

```
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
```

```
U - Per-user Static route
```

```
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
B 3.3.3.3/32 [200/0] via 33.33.33.33, label 5120, 01:04:26, vlan3
    10.1.2.2 [2], label 3, vlan3
```

```
PE1#show mpls forwarding-table
```

```
Pro: L - LDP, B - MP-BGP, R - RSVP, M - Mapped-Route, ML - mLDP (ML FEC: Root
address/OT/OV), RM - RSVP P2MP (RM FEC: P2MP ID/TID)
```

```
S - Static Label
```

Pro	Ident	FEC	Inlabel	Outlabel	Outgoing	Next hop
B	1	0.0.0.0/0	5120	/	/	/

It is indicated that the route label information of VPN1 exists in the forwarding table of PE1.

---

 **Note**

- The inspection method on PE2 and PE3 is the same as PE1.
- 

#Ping the loopback ports of CE1 and CE2 on CE3.

```
CE3#ping 1.1.1.1
```

```
Press key (ctrl + shift + 6) interrupt it.
```

```
Sending 5, 76-byte ICMP Echos to 1.1.1.1 , timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100% (5/5). Round-trip min/avg/max = 0/3/16 ms.
```

```
CE3#ping 2.2.2.2
```

```
Press key (ctrl + shift + 6) interrupt it.
```

```
Sending 5, 76-byte ICMP Echos to 2.2.2.2 , timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100% (5/5). Round-trip min/avg/max = 0/0/0 ms.
```

It is indicated that CE3 is able to ping through the loopback ports of CE1 and CE2.

#Ping the loopback port of CE2 on CE1.

```
CE1#ping 2.2.2.2
```

```
Press key (ctrl + shift + 6) interrupt it.
```

```
Sending 5, 76-byte ICMP Echos to 2.2.2.2 , timeout is 2 seconds:
```

```
.....
```

```
Success rate is 0% (0/5).
```

It is indicated that CE1 cannot ping through the loopback port of CE2.

# 80 MPLS OAM

---

## 80.1 MPLS OAM Introduction

The MPLS OAM function is used to implement fault detection and maintenance in MPLS networks, where MPLS LSP Ping/Traceroute are two common means to detect end-to-end LSP connectivity and control plane and data plane consistency.

## 80.2 MPLS OAM Function Configuration

Table 1-2 MPLS OAM Function Configuration List

Configuration Task	
Configure the MPLS OAM Function.	Enable the MPLS OAM Function
Check LSP	MPLS LSP Ping Function
	MPLS LSP Ping Function
	Interactive mode MPLS LSP Ping function
	Interaction Mode MPLS LSP Traceroute Feature

### 80.2.1 Configure the MPLS OAM Function.

#### Configuration Condition

Before configuring the MPLSOAM feature, do the following:

- Configure basic functions of MPLS to ensure that MPLS packets can be sent and received normally.

### Enable the MPLS OAM Function

Table 3-4 Enable the MPLS OAM Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable the MPLS OAM Function	<b>mpls oam</b>	Mandatory By default, the MPLS OAM function is not enabled

## 80.2.2 Check LSP

### Configuration Condition

To ensure the validity of the test results, the following tasks need to be completed prior to testing the LSP:

- When using MPLS LSP Ping detection, the MPLS OAM feature needs to be enabled on the Ingress node and Egress node of the LSP.
- When using MPLS LSP Traceroute detection, the MPLS OAM feature needs to be enabled on all nodes on the LSP path.

### MPLS LSP Ping Function

MPLS LSP Ping detects the connectivity of LSPs by sending and receiving Echo Request and Echo Reply packets. The Echo Request packet sent by the Ingress node carries the label corresponding to the arrival of the specified FEC, and the packet is sent to the Egress node through the detected LSP, which processes and returns the Echo Reply packet. If the Ingress node receives an Echo Reply packet without error information, the detected LSP is reachable; if no corresponding Echo Reply packet is received or an Echo Reply packet carrying an error TLV is received, the detected LSP is not reachable.

Table 5-6 MPLS LSP Ping Function

Step	Command	Description
Ping detection of LSP connectivity	<b>ping mpls</b> [ { <b>ipv4</b> <i>prefix-address prefix-mask-length</i> [ <b>destination</b> <i>address-start address-end address-increment</i> ]   <b>vrf</b> <i>vrf-name</i> <b>ipv4</b> <i>prefix-address prefix-mask-length</i> [ <b>destination</b> <i>address-start address-end address-increment</i> ] } [ <b>ttl</b> <i>time-to-live</i> / <b>source</b> <i>source-address</i> / <b>repeat</b> <i>count</i> / <b>timeout</b> <i>seconds</i> / <b>size</b> <i>packet-size</i> / <b>sweep</b> <i>minimum-size maximum-size size-increment</i> / <b>pad</b> <i>pattern</i> / <b>reply-pad-tlv</b> / <b>reply-mode</b> { <b>ipv4</b>   <b>router-alert</b> } / <b>interval</b> <i>msec</i> / <b>exp</b> <i>exp-bits</i> / <b>verbose</b> ] ]	Mandatory

### MPLS LSP Traceroute Function

MPLS LSP Traceroute is used to check the reachability and label consistency of each hop on the LSP path. The Ingress node sends Echo Request packets by increasing the TTL one by one and receives Echo Reply packets returned by each hop on the LSP path, thus discovering the information of each hop on the LSP path until it reaches Egress.

Table 7-8 MPLS LSP Traceroute Function

Step	Command	Description
Detection of reachability and label consistency for each hop on the LSP path	<b>traceroute mpls</b> [ { <b>ipv4</b> <i>prefix-address prefix-mask-length</i> [ <b>destination</b> <i>address-start address-end address-increment</i> ]   <b>vrf</b> <i>vrf-name</i> <b>ipv4</b> <i>prefix-address prefix-mask-length</i> [ <b>destination</b> <i>address-start address-end</i>	Mandatory

Step	Command	Description
	<i>adderss-increment</i> } } [ <b>ttl</b> <i>max-hop-count</i> / <b>source</b> <i>source-address</i> / <b>timeout</b> <i>seconds</i> / <b>reply-pad-tlv</b> / <b>reply-mode</b> { <b>ipv4</b>   <b>router-alert</b> } / <b>exp</b> <i>exp-</i> <i>bits</i> ] ]	

### Interactive mode MPLS LSP Ping function

Table 9-10 Interactive Mode MPLS LSP Ping Function

Step	Command	Description
Enter ping mpls interactive mode	<b>ping mpls</b>	Mandatory
Specify the type of FEC being detected	<b>Target ipv4 or vrf [ipv4]:</b> [ <b>ipv4</b>   <b>vrf</b> ]	Mandatory By default, the FEC type is ipv4
Specify the IPv4 address of the FEC being detected	<b>Target IPv4 address:</b> { <i>prefix-address</i> }	Mandatory
Specify the IPv4 mask length of the FEC being detected	<b>Target mask length [32]:</b> [ <i>prefix-mask-length</i> ]	Optional By default, the IPv4 mask length is 32
Specify the number of times the same MPLS echo request packet is sent repeatedly.	<b>Repeat count [5]:</b> [ <i>count</i> ]	Optional By default, the packet is sent 5 times repeatedly.
Specify the length of the MPLS echo request packet.	<b>Datagram size [120]:</b> [ <i>packet-size</i> ]	Optional By default, the packet length is 120 bytes.

Step	Command	Description
Specify the timeout for MPLS echo request packets.	<b>Timeout in seconds [2]:</b> [ <i>seconds</i> ]	Optional By default, the timeout time is 2 seconds
Specify the interval for sending MPLS echo request packets.	<b>Send interval in msec [0]:</b> [ <i>msec</i> ]	Optional By default, the sending interval of MPLS echo request packet is 0 milliseconds.
Select whether to enable the MPLS OAM function extension option.	<b>Extended command? [no]:</b> [ <i>yes   no</i> ]	Optional By default, the extension option is not enabled.
Specify the starting address for sending MPLS echo request packets with an incremental destination IPv4 address.	<b>Destination address or destination start address [127.0.0.1]:</b> [ <i>address-start</i> ]	Optional By default, the destination address for sending MPLS echo request packets is not incremental and is fixed at 127.0.0.1.
Specify the end address of the MPLS echo request packet sent with an incremental destination IPv4 address.	<b>Destination end address:</b> [ <i>address-end</i> ]	Optional
Specify the address increment value for sending MPLS echo request packets with incremental destination IPv4 addresses.	<b>Destination address increment [0.0.0.1]:</b> [ <i>address-increment</i> ]	Optional By default, the incremental value is 0.0.0.1.
Specify the IPv4 source address of the MPLS echo request packet.	<b>Source address:</b> [ <i>source-address</i> ]	Optional

Step	Command	Description
Specify the value of the EXP field in the MPLS label of the MPLS echo request packet.	<b>EXP bits in mpls header</b> [0]: [ <i>exp-bits</i> ]	Optional By default, the value of the EXP field in the label is 0.
Specify the padding value in the pad TLV of the MPLS echo request packet.	<b>Pad TLV pattern</b> [0xABCD]: [ <i>pattern</i> ]	Optional By default, the padding value in the pad TLV is 0xABCD.
Specifies whether the pad TLV is included in the MPLS echo reply packet.	<b>Reply Pad TLV?</b> [no]: [ <b>yes</b>   <b>no</b> ]	Optional By default, no pad TLV is included in the MPLS echo reply packet.
Set the TTL value of the outermost label of the MPLS echo request packet.	<b>Time To Live</b> [255]: [ <i>time-to-live</i> ]	Optional By default, the TTL value of the outermost label is 255.
Specify the reply mode of the MPLS echo reply packet.	<b>Reply mode (2-ipv4 via udp, 3-ipv4 via udp with router alert))</b> [2]:	Optional By default, the reply mode is 2, i.e., returned as IPv4 UDP packets.
Select whether to display the results of MPLS LSP Ping operations in detail mode.	<b>Verbose mode?</b> [no]: [ <b>yes</b>   <b>no</b> ]	Optional By default, the result of MPLS LSP Ping operation is displayed in abbreviated mode
Select whether to send MPLS echo request packets in incremental length	<b>Sweep range of sizes?</b> [no]: [ <b>yes</b>   <b>no</b> ]	Optional By default, MPLS echo request packets are sent in a fixed packet length

Step	Command	Description
Specify the starting value for sending the length of MPLS echo request packets.	<b>Sweep min size [120]:</b> [ <i>minimum-size</i> ]	Optional By default, the starting value of packet length is 120 bytes
Specify the maximum length of the transmitted MPLS echo request packet.	<b>Sweep max size [18024]:</b> [ <i>maximum-size</i> ]	Optional By default, the maximum value of incremental packet length is 18024 bytes.
Specify the incremental length of the MPLS echo request packet to be sent.	<b>Sweep interval [100]:</b> [ <i>size-increment</i> ]	Optional By default, the length increment value is 100 bytes

#### Interaction Mode MPLS LSP Traceroute Feature

Table 11-12 Interaction Mode MPLS LSP Traceroute Feature

Step	Command	Description
Enter traceroute mpls interactive mode	<b>traceroute mpls</b>	Mandatory
Specify the type of FEC being detected	<b>Target ipv4 or vrf [ipv4]:</b> [ <i>ipv4</i>   <i>vrf</i> ]	Mandatory By default, the FEC type is ipv4
Specify the IPv4 address of the FEC being detected	<b>Target IPv4 address:</b> { <i>prefix-address</i> }	Mandatory
Specify the IPv4 mask length of the FEC being detected	<b>Target mask length [32]:</b> [ <i>prefix-mask-length</i> ]	Optional By default, the IPv4 mask length is 32

Step	Command	Description
Specify the timeout for MPLS echo request packets.	<b>Timeout in seconds [2]:</b> [ <i>seconds</i> ]	Optional By default, the timeout time is 2 seconds
Select whether to enable the MPLS OAM function extension option.	<b>Extended command? [no]:</b> [ <i>yes</i>   <i>no</i> ]	Optional By default, the extension option is not enabled.
Specify the starting address for sending MPLS echo request packets with an incremental destination IPv4 address.	<b>Destination address or destination start address [127.0.0.1]:</b> [ <i>address-start</i> ]	Optional By default, the destination address for sending MPLS echo request packets is not incremental and is fixed at 127.0.0.1.
Specify the end address of the MPLS echo request packet sent with an incremental destination IPv4 address.	<b>Destination end address:</b> [ <i>address-end</i> ]	Optional
Specify the address increment value for sending MPLS echo request packets with incremental destination IPv4 addresses.	<b>Destination address increment [0.0.0.1]:</b> [ <i>address-increment</i> ]	Optional By default, the incremental value is 0.0.0.1.
Specify the IPv4 source address of the MPLS echo request packet.	<b>Source address:</b> [ <i>source-address</i> ]	Optional
Specify the value of the EXP field in the MPLS label of the MPLS echo request packet.	<b>EXP bits in mpls header [0]:</b> [ <i>exp-bits</i> ]	Optional By default, the value of the EXP field in the label is 0.

Step	Command	Description
Specifies whether the pad TLV is included in the MPLS echo reply packet.	<b>Reply Pad TLV? [no]: [ yes   no ]</b>	Optional By default, no pad TLV is included in the MPLS echo reply packet.
Set the TTL value of the outermost label of the MPLS echo request packet.	<b>Time To Live [30]: [ max-hop-count ]</b>	Optional By default, the maximum value of TTL increment for the outermost label is 30.
Specify the reply mode of the MPLS echo reply packet.	<b>Reply mode (2-ipv4 via udp) [2]:</b>	Optional

## 80.3 MPLS OAM Typical Configuration Example

### 80.3.1 Configure LSP Ping

#### Network Requirements

- In MPLS L3VPN networks, the reachability of MPLS LSPs is checked by using LSP Ping.

#### Network Topology

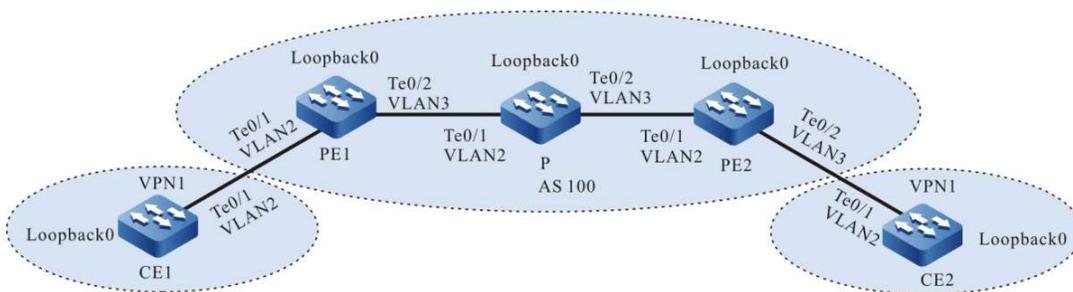


Figure 80-1 Network Topology for Configuring the LSP Ping

Table 13-14 Interface Mapping Relationships

of equipment	Interface	IP address	of equipment	Interface	IP address
CE1	Vlan2	10.1.1.1/24	P	Loopback0	22.22.22.22/32
	Loopback0	1.1.1.1/32	PE2	Vlan2	10.1.3.2/24
PE1	Vlan2	10.1.1.2/24		Vlan3	10.1.4.1/24
	Vlan3	10.1.2.1/24		Loopback0	33.33.33.33/32
	Loopback0	11.11.11.11/32	CE2	Vlan2	10.1.4.2/24
P	Vlan2	10.1.2.2/24		Loopback0	2.2.2.2/32
	Vlan3	10.1.3.1/24			

### Configuration Steps

Step 1: Configure the VLAN and add the port to the corresponding VLAN in access mode.  
(Omitted)

Step 2: Configure the IP address of each interface, CE1, PE1, P and PE2, CE2 form an MPLS L3VPN network, CE1 and CE2 can interoperate, and the VRF on PE1 is 1. (Omitted. Refer to the relevant section on MPLS L3VPN in the Configuration manual).

Step 3: Configure MPLS OAM on the Ingress node and Egress node of the LSP being detected.

#Configure MPLS OAM on PE1.

```
PE1#configure terminal
PE1(config)#mpls oam
```

#Configure MPLS OAM on PE1.

```
PE2#configure terminal
PE2(config)#mpls oam
```

Step 4: Check the result.

# LSP Ping operation on PE.

Take PE1 as an example:

```
PE1#ping mpls ipv4 33.33.33.33 32
```

Sending 5, 120-byte MPLS Echos to 33.33.33.33/32, TTL is 255, timeout is 2 seconds:

Codes: '!' - success, 'Q' - request not transmitted,  
'.' - timeout, 'U' - unreachable,  
'R' - downstream router but not destination,  
'M' - malformed request,  
'MR' - malformed reply

Press key (ctrl + shift + 6) to abort.

!!!!

Success rate is 100% (5/5), round-trip min/avg/max = 0/0/0 ms.

It is indicated that when PE1 pings PE2's loopback0 interface, PE1 continuously sends five echo request packets to the egress LSR PE2 and successfully receives the echo reply packets from PE2.

```
PE1#ping mpls vrf 1 ipv4 2.2.2.2 32
```

Sending 5, 120-byte MPLS Echos to vrf 1 2.2.2.2/32, TTL is 255, timeout is 2 seconds:

Codes: '!' - success, 'Q' - request not transmitted,  
'.' - timeout, 'U' - unreachable,  
'R' - downstream router but not destination,  
'M' - malformed request,  
'MR' - malformed reply

Press key (ctrl + shift + 6) to abort.

!!!!

Success rate is 100% (5/5), round-trip min/avg/max = 0/3/16 ms.

It is indicated that when PE1 pings CE2's loopback0 interface, PE1 continuously sends five echo request packets to CE2 and successfully receives the echo reply packets from CE2.

---

## Note

- Refer to PE1 for the inspection method on PE2.
-

## 80.3.2 Configure LSP Traceroute

### Network Requirements

- In MPLS L3VPN networks, MPLS LSP reachability is detected and each hop on the LSP path is discovered by using LSP Traceroute.

### Network Topology

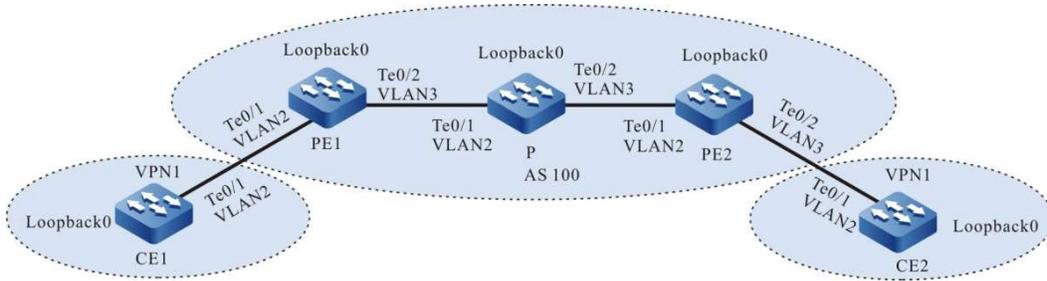


Figure 80-2 Network Topology for Configuring LSP Traceroute

Table 15-16 Interface Mapping Relationships

of equipment	Interface	IP address	of equipment	Interface	IP address
CE1	Vlan2	10.1.1.1/24	P	Loopback0	22.22.22.22/32
	Loopback0	1.1.1.1/32	PE2	Vlan2	10.1.3.2/24
PE1	Vlan2	10.1.1.2/24		Vlan3	10.1.4.1/24
	Vlan3	10.1.2.1/24		Loopback0	33.33.33.33/32
	Loopback0	11.11.11.11/32	CE2	Vlan2	10.1.4.2/24
P	Vlan2	10.1.2.2/24		Loopback0	2.2.2.2/32
	Vlan3	10.1.3.1/24			

### Configuration Steps

- Step 1: Configure the VLAN and add the port to the corresponding VLAN in access mode.  
(Omitted)

Step 2: Configure the IP address of each interface, CE1, PE1, P and PE2, CE1 and CE2 form an MPLS L3VPN network, CE1 and CE2 can interoperate, and the VRF on PE1 is 1. (Omitted. Refer to the relevant section on MPLS L3VPN in the Configuration manual).

Step 3: Configure MPLS OAM on all nodes through which the LSP being detected passes.

#Configure MPLS OAM on PE1.

```
PE1#configure terminal
PE1(config)#mpls oam
```

#Configure MPLS OAM on P.

```
P#configure terminal
P(config)#mpls oam
```

#Configure MPLS OAM on PE2.

```
PE2#configure terminal
PE2(config)#mpls oam
```

Step 4: Check the result.

#LSP Traceroute operation on each PE, CE.

Take PE1 as an example:

```
PE1#traceroute mpls ipv4 33.33.33.33 32
```

```
Tracing MPLS Label Switched Path to 33.33.33.33/32, timeout is 2 seconds:
```

```
Codes: '!' - success, 'Q' - request not transmitted,
        '!' - timeout, 'U' - unreachable,
        'R' - downstream router but not destination,
        'M' - malformed request,
        'MR' - malformed reply
```

```
Press key (ctrl + shift + 6) to abort.
```

```
0 10.1.2.1 mtu 1500 [Labels: 17 EXP: 0]
R 1 10.1.2.2 mtu 1500 [Labels: 3 EXP: 0] 0 ms
! 2 10.1.3.2 0 ms
```

It is indicated the path of the packet forwarded from PE1 to PE2 Loopback0 address and the label information of each hop.

```
PE1#traceroute mpls vrf 1 ipv4 2.2.2.2 32
```

Tracing MPLS Label Switched Path to vrf 1 2.2.2.2/32, timeout is 2 seconds:

Codes: '!' - success, 'Q' - request not transmitted,  
'.' - timeout, 'U' - unreachable,  
'R' - downstream router but not destination,  
'M' - malformed request,  
'MR' - malformed reply

Press key (ctrl + shift + 6) to abort.

```
0 10.1.2.1 mtu 1500 [Labels: 17/5120 EXP: 0/0]
R 1 10.1.2.2 mtu 1500 [Labels: 3/5120 EXP: 0/0] 0 ms
! 2 10.1.3.2 0 ms
```

It is indicated the path of the packet forwarded from PE1 to CE2 Loopback0 address and the label information of each hop.

---

## Note

- Refer to PE1 for the inspection method on PE2.
- 

# 81 ARP Check

---

## 81.1 Overview

ARP Check is used to check the legality of ARP packets so as to prevent illegal ARP packets from passing and improve network security.

The legality of ARP packets is checked according to the entries bound to the port, including the two types below:

Static binding entries manually configured;

Dynamic binding entries, dynamically generated by the valid entries of DHCP Snooping function and 802.1 function.

The specific detection principle of ARP Check is shown below:

For the ARP packets received by the port, if the IP address of sending end and source MAC address fully match the entries bound to the ARP Check of the port upon check, these ARP packets are legal and forwarded; otherwise, they are illegal and discarded.

## 81.2 ARP Check Function Configuration

Table 81-1 ARP Check Function Configuration List

Configuration Task	
Enable ARP Check Function of the Port	Enable ARP Check Function of the Port
Configure Binding Static Entries of ARP Check	Configure Binding Static Entries of ARP Check
Configure to Reinstall the Entries Failed in Writing Hardware	Configure to Reinstall the Entries Failed in Writing Hardware

### 81.2.1 Enable ARP Check Function of the Port

#### Configuration Condition

None

#### Enable ARP Check Function of the Port

After enabling the ARP Check function of the port, ARP Check will dynamically obtain entries from the DHCP Snooping database and write ACL hardware.

Table 1 Configuring Enabling ARP Check Function of the Port

Step	Command	Description
Enter the global configuration mode.	<b>config terminal</b>	-

Step	Command	Description
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Enable ARP check function of the port	<b>arp-check enable</b>	Mandatory  By default, the ARP Check function of the port is disabled.

## 81.2.2 Configure Binding Static Entries of ARP Check

### Configuration Condition

None

### Configure Binding Static Entries of ARP Check

Table 81-3 Configuring Binding Static Entries of ARP Check

Step	Command	Description
Enter the global configuration mode.	<b>config terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	

Step	Command	Description
		enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Configure Binding Static Entries of ARP Check	<b>arp-check binding</b> <i>mac-address ip-address</i> <b>rate limit-value</b>	Mandatory  By default, no static binding entry of ARP Check is configured.

### 81.2.3 Configure to Reinstall the ARP Check Entries Failed in Writing Hardware

#### Configuration Condition

None

#### Configure to Reinstall the ARP Check Entries Failed in Writing Hardware

Table 81-4 Configuring to Reinstall ARP Check Entries Failed in Writing Hardware

Step	Command	Description
Enter the global configuration mode.	<b>config terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	

Step	Command	Description
Configure to reinstall the entries failed in writing hardware.	<b>arp-check install</b>	Mandatory By default, the port doesn't automatically install the hardware entries failed in writing.

## 81.2.4 ARP Check Monitoring and Maintaining

Table 81-5 ARP Check Monitoring and Maintaining

Command	Description
<b>show arp-check</b> [ <b>active</b>   <b>brief</b>   <b>inactive</b>   <b>interface</b> <i>interface-name</i>   <b>interface link-aggregation</b> <i>link-aggregation-id</i> ]	A command used to show the information in ARP Check entries

## 81.3 Typical Configuration Example of ARP Check

### 81.3.1 Configure Basic Functions of ARP Check

#### Network Requirements

- PC1 and PC2 access IP network through the Device;
- Configure the basic functions of ARP Check so that PC1 instead of PC2 can normally access the IP Network.

#### Network Topology

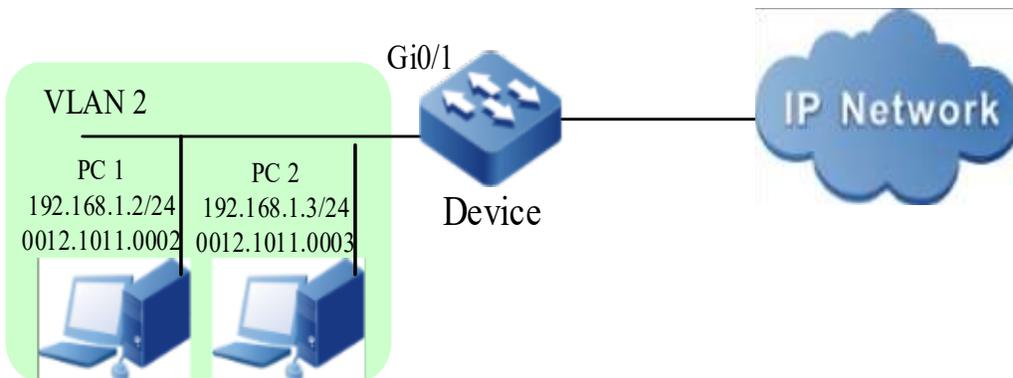


Figure 1 Network Topology for Configuring Basic Functions of ARP Check

### Configuration Steps

Step 1: Configure VLAN and port link type on Device.

#Create VLAN 2.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the link type of port gigabitethernet0/1 as Access to allow services of VLAN 2 to pass.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode access
Device(config-if-gigabitethernet0/1)#switchport access vlan 2
Device(config-if-gigabitethernet0/1)#exit
```

Step 2: Configure ARP Check function on Device.

#Enable the ARP Check function on port gigabitethernet0/1, and configure ARP Check binding entries with MAC address of 0012.1011.0002 and IP address of 192.168.1.2.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#arp-check enable
Device(config-if-gigabitethernet0/1)#arp-check binding 0012.1011.0002 192.168.1.2 rate 10
Device(config-if-gigabitethernet0/1)#exit
```

Step 3: Check the result.

#View ARP Check-related configuration information.

```
Device#show arp-check brief
-----
Interface Name  Status  Binding Table
-----
gi0/1          Enable  Yes
```

It is indicated that the port gigabitethernet0/1 has enabled the ARP Check function and has ARP Check entries.

# View ARP Check binding entries of the port.

```
Device#show arp-check interface gigabitethernet0/1
-----ARP Check Table-----
Interface-Name  Status  MAC-Address  IP-Address  Rate  PolicySource  SetHardware
-----
gi0/1           enable  0012.1011.0002  192.168.1.2  10  STATIC       active
total number: 1
```

#PC1 instead of PC2 can normally access the IP Network.

### 81.3.2 Combination of ARP Check with DHCP Snooping

#### Network Requirements

- PC1 which uses static IP address and PC2 which obtains IP address through DHCP access the IP Network through the Device;
- Configure DHCP Snooping and ARP Check function for the Device so that PC2 instead of PC1 can normally access the IP Network.

#### Network Topology

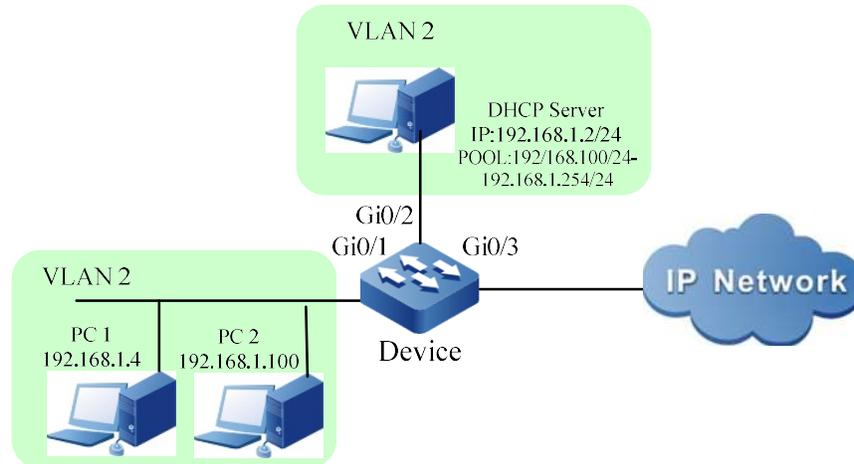


Figure 2 Network Topology for Combination of ARP Check and DHCP Snooping

### Configuration Steps

Step 1: Configure VLAN and port link type on Device.

#Create VLAN 2.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the link type of the ports gigabitethernet0/1, gigabitethernet0/2 and gigabitethernet0/3 as Access, permitting the services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/1-0/3
Device(config-if-range)#switchport access vlan 2
Device(config-if-range)#exit
```

Step 2: Configure DHCP Snooping function on Device.

#Enable the DHCP Snooping function and configure gigabitethernet0/2 as a trusted port.

```
Device(config)#dhcp-snooping
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#dhcp-snooping trust
Device(config-if-gigabitethernet0/2)#exit
```

Step 3: Configure ARP Check function on Device.

#Enable the ARP Check function on the port gigabitethernet0/1.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#arp-check enable
Device(config-if-gigabitethernet0/1)#exit
```

Step  
4: Check the result.

#After PC2 successfully obtains the IP address, view the dynamic entries of DHCP Snooping on the Device.

```
Device#show dhcp-snooping database
dhcp-snooping database:
database entries count:1
database entries delete time :300
-----
macAddr      ipAddr      transtion-id  vlan  interface      leaseTime(s)  status
0013.0100.0001  192.168.1.100  2            2     gi0/1          107990        active
-----
```

#View ARP Check binding entries of the port gigabitethernet0/1.

```
Device#show arp-check interface gigabitethernet0/1
-----ARP Check Table-----
Interface-Name  Status  MAC-Address  IP-Address  Rate  PolicySource  SetHardware
-----
gi0/1          enable  0013.0100.0001  192.168.1.100  16  DHCPSP      active
total number: 1
```

#PC2 instead of PC1 can normally access the IP Network.

### 81.3.3 Combination of ARP Check with 802.1X

#### Network Requirements

- PC1 accesses IP network through the Device which uses 802.1X access control;
- RADIUS authentication is used as an authentication method;
- PC1 cannot access network without successful authentication. It is permitted to access the IP Network once it passes the authentication;
- After the successful authentication, users can generate ARP Check entries to check the legality of their ARP packets.

#### Network Topology

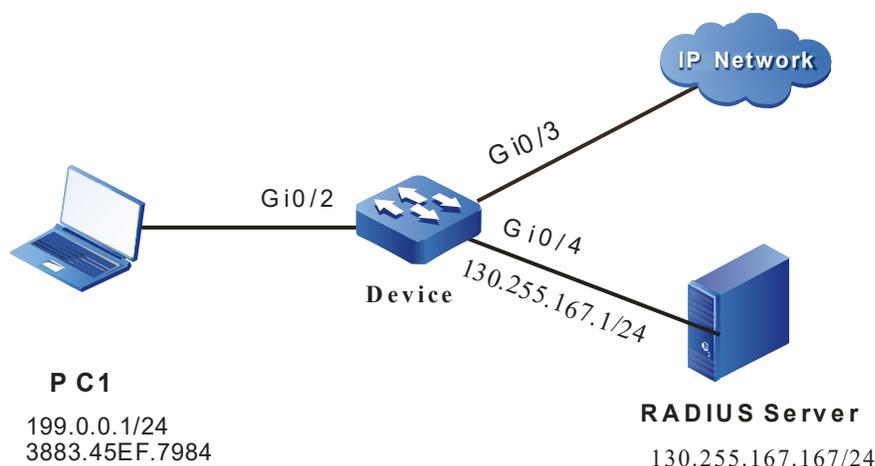


Figure 3 Network Topology for Combination of ARP Check and 802.1X

### Configuration Steps

Step 1: Configure VLAN and port link type on Device.

#Create VLAN2~VLAN4 on Device.

```
Device#configure terminal
Device(config)#vlan 2-4
Device(config)#exit
```

#Configure the link type of the port gigabitethernet 0/2 as Access to allow services of VLAN 2 to pass.

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport access vlan 2
Device(config-if-gigabitethernet0/2)#exit
```

#Configure the link type of the ports gigabitethernet 0/3~gigabitethernet 0/4 on the Device as Access, allowing the services of VLAN3~VLAN4 to pass. (Omitted)

Step 2: Configure interface IP address for Device.

#Configure the IP address of VLAN4 as 130.255.167.1/24.

```
Device(config)#interface vlan 4
Device(config-if-vlan4)#ip address 130.255.167.1 255.255.255.0
Device(config-if-vlan4)#exit
```

Step 3: Configure AAA authentication.

#Enable AAA authentication on Device, authentication method RADIUS, server key admin, priority 1, and RADIUS server address 130.255.167.167/24.

```
Device(config)#domain system
```

```
Device(config-isp-system)# aaa authentication dot1x radius-group radius
Device(config-isp-system)#exit
Device(config)#aaa server group radius radius
Device(config-sg-radius-radius)#server 130.255.167.167 priority 1 key admin
```

Step 4: Configure AAA server.

#On AAA server, configure user name, password and key value as admin. (Omitted)

Step 5: Configure 802.1X authentication.

#Enable 802.1X authentication on the port and configure the authentication mode as Macbased.

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#dot1x port-control enable
Device(config-if-gigabitethernet0/2)# authentication port-method macbased

Device(config-if-gigabitethernet0/2)#exit
```

Step 6: Configure ARP Check function on the Device.

#Enable the ARP Check function on the port gigabitethernet0/2.

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#arp-check enable
Device(config-if-gigabitethernet0/2)#exit
```

Step 7: Authentication succeeds.

#Before passing the authentication, PC1 cannot access the network.

#After PC1 users initiate authentication and the authentication succeeds, PC1 can access the IP network.

```
Device#show dot1x user
-----
NO 1 : MAC_ADDRESS= 3883.45ef.7984 STATUS= Authorized USER_NAME= admin
      VLAN= 2 INTERFACE= gi0/2 USER_TYPE= DOT1X
      AUTH_STATE= AUTHENTICATED BACK_STATE= IDLE IP_ADDRESS= 199.0.0.1
      IPV6_ADDRESS= Unknown

      Online time: 0 week 0 day 0 hours 0 minute 51 seconds

Total: 1 Authorized: 1 Unauthorized/guest/critical: 0/0/0 Unknown: 0
```

Step 8: Check the result.

```

Device#show arp-check interface gigabitethernet0/2
-----ARP Check Table-----
Interface-Name Status MAC-Address IP-Address Rate PolicySource SetHardware
-----
gi0/2          enable 3883.45ef.7984 199.0.0.1 16 DOT1X active

total number: 1

```

#If the APR packets and entries sent by PC1 can be fully matched, they can be normally forwarded and limited in speed; otherwise, they will be directly discarded.

# 82 CPU Protection

---

## 82.1 Overview

There are lots of protocol packets in the device that need to be sent to CPU for processing and we need to specify the queue for each kind of protocol packets. The CPU protection function classifies the protocol packets sent to CPU and the packets enter different CPU queues according to the different protocol priorities. We can set the rate limitation of each queue.

The device totally has eight queues, numbering from 0 to 7. They adopt the strict priorities. The smaller the number is, the lower the priority is. That is to say, the priority of queue 0 is the lowest and the priority of queue 7 is the highest. The packets in the queue with the high priority are earlier sent to the CPU for processing than the packets in the queue with low priority. We can specify them to different priorities of queues according to the importance of each kind of packets, ensuring that the important packets are first sent to the CPU for processing.

Meanwhile, the device can perform the rate limitation for the packets entering each CPU queue, preventing the vicious protocol packet attack in the network from causing the too high CPU utilization of the device and resulting in the abnormal running of the device.

## 82.2 Configure CPU protection function

Table 82 CPU Protection Function Configuration List

Configuration Task	
Configure CPU Queue of Protocol Packets	Configure CPU Queue of Protocol Packets
Configure Rate Limitation of CPU Queue	Configure Total Rate Limitation of All CPU Queues
	Configure Rate Limitation of Each CPU Queue
Make Users' Custom Protocol Packets Delivered to CPU for Processing	Configure the Match Rules of Delivering Users' Custom Protocol Packets to CPU for Processing
	Configure the Method of Delivering Users' Custom Protocol Packets to CPU for Processing

### 82.2.1 Configure CPU Queue of Protocol Packets

#### Configuration Condition

None

#### Configure CPU Queue of Protocol Packets

The device has 8 CPU queues. Users can configure to make different protocol packets enter different queues. The device can deliver protocol packets to CPU for processing by the priority of queues from high to low according to user's configuration. The protocol packets in the queue with a high priority will be first delivered to CUP for processing. Users can specify important packets to enter the queue with a high priority so that they can be first delivered to CUP for processing. By default, different protocol packets enter default CPU queues or the specified CPU queue through a command.

Table 1 Configuring CPU Queue of Protocol Packets

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure CPU Queue of Protocol Packets	<b>cpu-packet protocol cos</b> <i>cos-value</i>	Mandatory By default, different protocol packets enter their default CPU queue.

## 82.2.2 Configure the Traffic rate Limitation of Protocol Packets

### Configuration Condition

None

### Configure the Committed Information Rate and Committed Burst Size of Protocol Packets

The device can monitor and control the traffic of vbrp, vrrp, and vrrp3 protocol packets. Users can limit the traffic size of specific protocol packets by configuring committed information rate and committed burst size. This can prevent a large number of continuous bursts of business data which will make the network more congested, or even network congestion to cause abnormal business.

Table 2 Configuring Committed Information Rate and Committed Burst Size of Protocol Packets

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the committed information rate and committed burst size of protocol packets	<b>cpu-packet { vbrp   vrrp   vrrp3 } cir cir-value cbs</b> <i>cbs-value</i>	Mandatory By default, default committed information rate and committed burst size are configured for different protocol packets.

## 82.2.3 Configure Total Rate Limitation of All CPU Queues

### Configuration Condition

None

### Configure Total Rate Limitation of All CPU Queues

Malicious network attack will make the device unable to operate due to a very high CPU utilization rate. In order to prevent this, users can configure the total rate limitation of all CPU queues. If any attack occurs, and the total packet rate of all the queues exceeds the total rate limitation, the packets will be discarded to avoid a very high CPU utilization rate.

Table 3 Configuring Total Rate Limitation of All CPU Queues

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure Total Rate Limitation of All CPU Queues	<b>cpu-packet cos global pps</b> <i>pps-value</i>	Mandatory By default, the total rate limit of all queues is 2000PPS.

### 82.2.4 Configure Rate Limitation of Each CPU Queue

#### Configuration Condition

None

#### Configure Rate Limitation of Each CPU Queue

Malicious network attack will make the device unable to operate due to a very high CPU utilization rate. In order to prevent this, users can configure the rate limitation of each CPU queue. If any attack occurs, and the packet rate in the queue exceeds the rate limit of this queue, the packets will be discarded to avoid a very high CPU utilization rate. By default, different rate limits are set for different CPU queues. Users may modify the rate limit as needed.

Table 4 Configuring Rate Limitation of Each CPU Queue

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Configure Rate Limitation of Each CPU Queue	<b>cpu-packet cos</b> <i>cos-value</i> <b>pps</b> <i>pps-value</i>	Mandatory By default, each queue has a unique rate limit.

## 82.2.5 Make Users' Custom Protocol Packets Delivered to CPU for Processing

### Configuration Condition

None

### Configure the Match Rules of Delivering Users' Custom Protocol Packets to CPU for Processing

The match rules of delivering users' custom protocol packets to CPU for processing must be used with the method of delivering users' custom protocol packets to CPU for processing. It will conduct corresponding action processing for the packets meeting the match rules. The match rules include `dst-mac` (destination MAC address), `ingress` (interface), `vlan-id` (VLAN number), `ether-type` (ether type), IP (IPV4), IPV6, 0x0000 (custom Ethernet type), `ip-protocol` (IP protocol, such as IGMP and TCP), `dst-ip` (destination IP), `src-port` (source port), and `dst-port` (destination port). Users can combine the match rules mentioned above as needed.

Table 5 Configuring the Match Rules of Delivering Users' Custom Protocol Packets to CPU

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the rules of matching users' custom protocol packets	<b>cpu-packet user-define</b> <i>user-id match { dst-mac</i> <i>dst-mac   ether-type</i> <i>{ ether-type-value   ip</i> <i>[ dst-ip dst-ip-address  </i> <i>dst-mac dst-mac   ingress</i> <i>ingress-interface   ip-</i> <i>protocol protocol-type  </i> <i>vlan-id vlan-id [ dst-ip dst-</i> <i>ip-address   ingress</i> <i>ingress-interface   ip-</i>	Mandatory By default, there are no match rules.

Step	Command	Description
	<pre> <b>protocol</b> <i>protocol-type</i> ] ]   <b>ipv6</b> [ <b>dst-ip6</b> <i>dst-ipv6- address</i>   <b>dst-mac</b> <i>dst-mac</i> / <b>ingress</b> <i>ingress-interface</i>   <b>ip-protocol</b> <i>protocol- type</i>   <b>vlan-id</b> <i>vlan-id</i> [ <b>dst- ip</b> <i>dst-ip-address</i>   <b>ingress</b> <i>ingress-interface</i>   <b>ip- protocol</b> <i>protocol-type</i> ] ] }   <b>ingress</b> <i>ingress-interface</i>   <b>vlan-id</b> <i>vlan-id</i> [ <b>ingress</b> <i>ingress-interface</i> ] } </pre>	

### Configure the Method of Delivering Users' Custom Protocol Packets to CPU for Processing

The match rules of delivering users' custom protocol packets to CPU for processing must be used with the method of delivering users' custom protocol packets to CPU for processing. It will conduct corresponding action processing for the packets meeting the match rules. For example, if the configuration method is copy, the original forwarding process of the packets will not be changed. Instead, the packets will be delivered to CPU for processing by copying. If the configuration method is drop, the packets are not permitted to be delivered to CPU for processing, but discarded. If the configuration method is remark, the priority of delivering packets to CPU for processing is modified. If the configuration method is trap, the original forwarding process of packets is changed. The packets are delivered to CPU for processing instead of being forwarded.

Table 6 Configuring Method of Delivering Users' Custom Protocol Packets to CPU

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the Method of Delivering Users' Custom Protocol Packets to CPU for Processing	<pre> <b>cpu-packet user-define</b> <i>user-id</i> <b>action</b> { <b>drop</b>   { <b>copy</b>   <b>remark</b>   <b>trap</b> } <b>cos</b> <i>cos-value</i> } </pre>	<p>Mandatory</p> <p>By default, no action processing is conducted for the packets meeting the match rules.</p> <p>When the method of delivering users' custom</p>

Step	Command	Description
		protocol packets to CUP for processing is copy, remark or trap, the cos value can be specified.

## 82.2.6 CPU Protection Monitoring and Maintaining

Table 7 CPU Protection Monitoring and Maintaining

Command	Description
<b>show cpu-packet protocol-config-table</b>	Show the configuration information of delivering all protocol packets to CPU
<b>show cpu-packet cos</b>	Show current and default queue information of delivering protocol packets to CPU for processing
<b>show cpu-packet pps</b>	Show the rate limitation information of each CPU queue
<b>show cpu-packet udf-table</b>	Show the information of users' all custom ACL entries set through CPU protection module

## 82.3 Typical Configuration Example of CPU Protection

### 82.3.1 Configure Basic Functions of CPU Protection

#### Network Requirements

- PC can access IP Network through the Device.
- Make DHCP packets enter queue 5 on the Device so that the DHCP protocol packets can be first processed by CPU.
- Limit the rate of the ARP queue on the Device so that the packets with a low priority

can be normally processed even if the Device has a very high CPU utilization rate.

## Network Topology

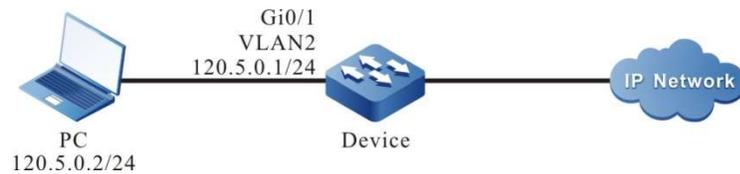


Figure 82 Network Topology for Configuring Basic Functions of CPU Protection

## Configuration Steps

Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configures IP addresses for the ports. (Omitted)

Step 3: Configure CPU queue of DHCP packets.

#Make DHCP packets enter queue 5 on the Device.

```
Device#configure terminal
Device(config)#cpu-packet dhcp cos 5
```

Step 4: Configure rate limitation of CPU queue.

#Configure the rate limit of CPU queue as 100pps on the Device.

```
Device(config)#cpu-packet cos 1 pps 100
```

Step 5: Check the result.

#View the CPU queue of each protocol packet on the Device.

```
Device#show cpu-packet cos
Type          Current-CoS  [Default-CoS]
-----
random        0            [0]
ipv6-all     0            [0]
pppoe         0            [0]
udp-broadcast 0            [0]
icmp          0            [0]
ip-e-packet   0            [0]
ip            0            [0]
mpls-unicast 0            [0]
mpls-multicast 0           [0]
```

LBD_l2-src-miss	0	[0]
ipaddr-0	0	[0]
ipaddr-127	0	[0]
ipv4-all	0	[0]
src-martian-addr	0	[0]
arp	1	[1]
ip6-solicited-node	1	[1]
host-group	1	[1]
router-group	1	[1]
ND	1	[1]
trill-oam	1	[1]
rarp	1	[1]
lldp	2	[2]
dot1x	2	[2]
dhcp	5	[2]
dhcpv6	2	[2]
http	2	[2]
svi-ip	2	[2]
vxlan	2	[2]
pim	3	[3]
pim6	3	[3]
igmp-dvmrp	3	[3]
ip6-interface-multicast	3	[3]
ike	3	[3]
ntp	3	[3]
mld	3	[3]
ekg	3	[3]
rsvp	4	[4]
ospf	4	[4]
ospfv3	4	[4]
irmp	4	[4]
rip	4	[4]
ripng	4	[4]
is-is	4	[4]
bgp	4	[4]
ldp	4	[4]
ipsec-esp	4	[4]
ipsec-ah	4	[4]
mlag-keep-alive	4	[4]
mvst	5	[5]
l2-interface-unicast	5	[5]
gvrp	5	[5]
mvst-inspection	5	[5]
ulfd	5	[5]
l2pt	5	[5]
svi-icmp	5	[5]
ethernet-cfm	5	[5]
ethernet-lmi	5	[5]
mlag-pts	5	[5]
mpls-oam	5	[5]
bfd	6	[6]
vbrp	6	[6]
vrrp	6	[6]
vrrp3	6	[6]
telnet	6	[6]
ssh	6	[6]
loopback-detect	6	[6]
slow-protocols	6	[6]
stp-bpdu	6	[6]
stp-vist	6	[6]
radius	6	[6]
trill	6	[6]
eips	7	[7]
ulpp	7	[7]

```

mad-fast-hello      7      [7]
erps                7      [7]
mlag                7      [7]
Device#

```

It is indicated that the CPU queue of DHCP on the Device is changed from the default queue 2 to queue 5.

#View the rate limit of each queue on the Device.

```

Device#show cpu-packet pps
CoS  Current-PPS  [Default-PPS]
-----
0    200           [200]
1    100           [250]
2    500           [500]
3    600           [600]
4    1000          [1000]
5    400           [400]
6    300           [300]
7    100           [100]
TOTAL 2000        [2000]

```

It is indicated that the rate limit of queue 1 where ARP is located on the Device is changed from the default 250pps to 100pps.

### 82.3.2 Configure Custom Rules of CPU Protection

#### Network Requirements

- Device is directly connected to PC1 and PC2 respectively.
- Configure the custom rules of CPU protection on the Device, and make the packets meeting the match conditions delivered to CPU for processing through trap and enter corresponding queue.

#### Network Topology

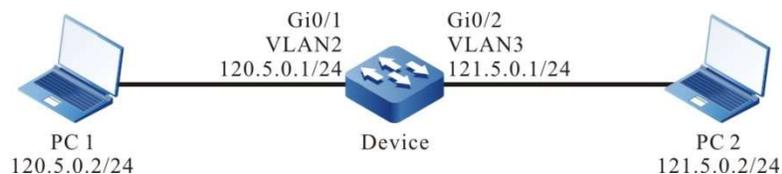


Figure 1 Network Topology for Configuring Custom Rules of CPU Protection

#### Configuration Steps

Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configures IP addresses for the ports. (Omitted)

Step 3: Configure custom rules of CPU protection.

#Configure the custom rules of CPU protection, and make the packets with a destination address of 121.5.0.2 delivered to CPU for processing in trap mode and set the COS value as 5.

```
Device#configure terminal
Device(config)#cpu-packet user-define 1 match ether-type ip dst-ip host 121.5.0.2
Device(config)#cpu-packet user-define 1 action trap cos 5
```

Step 4: Check the result.

#View custom rules on the Device.

```
Device#show cpu-packet udf-table
user-define 1
ether-type: 0x0800(IPv4)
dst-ip: host 121.5.0.2
location: global
valid: yes
action: trap
CoS: 5
```

#When PC1 accesses PC2, the custom rules of CPU protection take effect. The packets with a destination address of 121.5.0.2 on the Device are delivered to CPU for processing in trap mode and enter queue 5.

---

### Note

- Please see this configuration when the custom rules match other conditions and execute other methods.
-

# 83 Port Security

---

## 83.1 Overview

### 83.1.1 Introduction

Port security is a security mechanism used to control the device assessed to the network. Generally applied in the access layer, it can limit the host using device ports and permits some specific hosts to access the network only.

The port security function flexibly binds four elements of the user, i.e. MAC address, IP address, VLAN ID, and port number, to prevent illegal users from accessing the network. This can ensure the network data are secure and valid users have enough bandwidth.

### 83.1.2 Port Security Rules

Port security rules can be classified into four types:

**MAC rules:** They control whether the host can communicate according to its MAC address. Their binding methods include MAC binding, MAC+VLAN binding, MAC+IP binding, and MAC+IPv6 binding;

**IP rules:** They control whether the host can communicate according to its IP address. IP rules can be bound to a single IP address or an IP address segment;

**IPv6 rules:** They control whether the host can communicate according to its IPv6 address. IPv6 rules can be bound to a single IPv6 address or an IPv6 address segment;

**MAX rules:** They control the communication of the host by limiting the number of MAC address entries that the port can freely learn. They don't include the legal MAC address entries generated by MAC rules, IP rules and IPv6 binding;

**STICKY rules:** They control whether the host can communicate according to its MAC address. Their binding methods include MAC binding, MAC+VLAN binding, MAC+IP binding, and MAC+IPv6 binding. STICKY rules can be both automatically learned and manually configured. They are saved in running configuration. If the running configuration is saved prior to restarting the device, these STICKY rules can take effect automatically after the device is restarted. When the STICKY function is enabled under the port and the

STICKY learning mode is MAC, the dynamic MAC entries learned by the MAX rules will be transformed into STICKY rules and saved in the running configuration;

VOICE VLAN rules: They control the communication of the host by identifying whether the MAC address belongs to the OUI configured by VOICE-VLAN. They don't include the legal MAC address entries generated by MAC rules, IP rules and IPv6 binding.

### 83.1.3 Working Principle of Port Security

If only port security is enabled, the port security will discard all the packets received on the port. The port security rules are triggered by the ARP packets and IP packets of the terminal device. When the device receives the ARP packets and IP packets, the port security extracts packet information from them, and matches them with the configured rules. The matching order is shown below: MAC rules, STICKY rules, IP rules, and MAX rules. It controls the layer-2 forwarding table of the port according to the matching result so as to control the port's behavior of forwarding packets. If the packets that match MAX rules or STICKY rules are legal, they will be forwarded. For the packets that match MAC rules or IP rules, if the action performed by the rule on the packet is permit, then the packet is legal and will be forwarded; otherwise, the packet is illegal and will be discarded.

For the MAC rules and IP rules with the action of permit, after they take effect, their corresponding MAC address is written into the layer-2 forwarding table so that the packets matching the rules can be forwarded in layer 2. For the MAC rules and IP rules with the action of reject, their corresponding MAC is not written into the layer-2 forwarding table, and the packets need to be discarded through port security.

After MAX rules and STICKY rules take effect, they are written into the MAC address entries to form valid entries so that the packets can be forwarded in layer 2. IPv6 packets are processed in similar ways.

## 83.2 Port Security Function Configuration

Table 83 Basic Function Configuration List of Port Security

Configuration Task	
Configure Basic Functions of Port Security	Enable Port Security Function
Configure Port Security Rules	Configure MAC Rules
	Configure IP Rules
	Configure IPv6 Rules
	Configure MAX Rules
	Configure STICKY Rules

Configuration Task	
	Configure VOICE VLAN Rules
Configure STICKY Rules Learning Mode	Configure STICKY Rules Learning Mode
Configure Static MAC Address Aging Function	Enable Static MAC Address Aging Function
	Configure Static MAC Address Aging Time
Configure Processing Mode After Receiving Illegal Packets	Configure Processing Mode After Receiving Illegal Packets
Configure Log Sending Interval After Receiving Illegal Packets	Configure Log Sending Interval After Receiving Illegal Packets
Configure Port Security to Use ACL Function	Configure Port Security to Use ACL Function

### 83.2.1 Configure Basic Functions of Port Security

In the various configuration tasks of port security, you must first enable port security so that the configuration of the other function features can take effect.

#### Configuration Condition

None

#### Enable Port Security Function

After port security is enabled, if no port security rule is configured, the port cannot learn MAC address.

Table 83 Configuring Basic Functions Port Security

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.

Step	Command	Description
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enable Port Security Function	<b>port-security enable</b>	Mandatory  By default, the port security function is not enabled.

---

### Note

- The IP rules and MAX rules of port security cannot be used with 802.1x on the same port.
  - The IP rules and MAX rules of port security cannot be used with MAC address authentication on the same port.
  - Port security cannot be used with the secure channel authentication function on the same port.
  - Port security cannot be used with DAI (Dynamic ARP Inspection) on the same port.
- 

## 83.2.2 Configure Port Security Rules

### Configuration Condition

Before configuring port security rules, ensure that:

- Enable the port security function.

### Configure MAC Rules

To control the communication of a terminal with MAC address, users may use MAC rules. The packets of the rules matching the action of permit can be forwarded, while those of the rules matching the action of reject will be discarded.

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Configure MAC rules with the action of permit	<b>port-security permit mac-address</b> <i>mac-address-value</i> [ <b>desc</b> <i>security-rule-description</i>   <b>ip-address</b> <i>ip-address-value</i> [ <b>desc</b> <i>security-rule-description</i> ]   <b>ipv6-address</b> <i>ipv6-address-value</i> [ <b>desc</b> <i>security-rule-description</i> ]   <b>vlan-id</b> <i>vlan-id</i> [ <b>desc</b> <i>security-rule-description</i> ] ]	At least one option must be selected.  By default, MAC rules are not configured under the port.
Configure MAC rules with the action of reject	<b>port-security deny mac-address</b> <i>mac-address-value</i> [ <b>ip-address</b> <i>ip-address-value</i>   <b>ipv6-address</b> <i>ipv6-address-value</i>   <b>vlan-id</b> <i>vlan-id</i> ]	

## Configure IP Rules

To control the communication of a terminal with IP address, users may use IP rules. The packets of the rules matching the action of permit can be forwarded, while those of the rules matching the action of reject will be discarded.

Table 2 Configuring IP Rules

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Configure IP rules with the action of permit	<b>port-security permit ip-address</b> <i>ip-address-value</i> [ <b>to</b> <i>ip-address-value</i> ]	At least one option must be selected.
Configure IP rules with the action of reject	<b>port-security deny ip-address</b> <i>ip-address-value</i> [ <b>to</b> <i>ip-address-value</i> ]	By default, IP rules are not configured under the port.

### Configure IPv6 Rules

To control the communication of a terminal with IPv6 address, users may use IP rules. The packets of the rules matching the action of permit can be forwarded, while those of the rules matching the action of reject will be discarded.

Table 3 Configuring IPv6 Rules

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.

Step	Command	Description
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Configure IPv6 rules with the action of permit	<b>port-security permit ipv6-address</b> <i>ipv6-address-value</i> [ <b>to</b> <i>ipv6-address-value</i> ]	At least one option must be selected.  By default, IPv6 rules are not configured under the port.
Configure IPv6 rules with the action of reject	<b>port-security deny ipv6-address</b> <i>ipv6-address-value</i> [ <b>to</b> <i>ipv6-address-value</i> ]	

### Note

Port security provides secure access in the data link layer. For the IPv6 rules currently supported like MAC+IPv6 and IPv6, once corresponding valid entries are generated, subsequent packets can be normally forwarded only if they match the MAC+VLAN entries that have been generated. Their IPv6 addresses are not checked.

### Configure MAX Rules

Under the port where port security function has been enabled, if users hope the terminal accessed can communicate event if it doesn't match the MAC rules and IP rules, they can configure MAX rules which will limit the number of terminals permitted to be access.

Table 4 Configuring MAX Rules

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Configure MAX Rules	<b>port-security maximum</b> <i>maximum-number</i>	Mandatory  By default, MAX rules permit the number of MAC addresses learned to be 0.

---

### Note

- The actual number of dynamic addresses learned by the MAX rules is limited by the number of ports, VLANs, and system MAC addresses.
- 

### Configure STICKY Rules

If users wish the MAC address and VLAN information corresponding to the terminal permitted by MAX rules are saved in the configuration, they can enable the STICKY function on the device so that the entries learned by the device through MAX rules can be transformed into STICKY rules. Upon completion of the transformation, the number of MAX rules can be adjusted by the number of current STICKY rules so that only the terminals that match STICKY rules can communicate. Then, the device can automatically learn the MAC address of the terminal accessed, transform it into STICKY rules, and save them in the configuration without manually configuring MAC rules.

Table 5 Configuring STICKY Rules

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Configure MAX Rules	<b>port-security maximum</b> <i>maximum-number</i>	Mandatory  By default, the number of dynamic MAC addresses that MAX rules permit to learn is 0. STICKY rules can be configured only after the number of MAX rules is configured.
Enable the STICKY function	<b>port-security permit mac-address sticky</b>	Mandatory  By default, the STICKY function is not enabled. STICKY rules can be configured only after the STICKY function is enabled.
Configure STICKY Rules	<b>port-security permit mac-address sticky</b> [ <i>mac-address-value</i> [ <b>desc</b> <i>security-rule-description</i> / <b>vlan-id</b> <i>vlan-id</i> [ <b>desc</b> <i>security-rule-description</i> ] ]   <b>ip-address</b> <i>ip-address-value</i> [ <b>desc</b> <i>security-rule-description</i> ]   <b>ipv6-address</b>	Mandatory  By default, STICKY rules are not configured under the port.

Step	Command	Description
	<code>ipv6-address-value [ desc security-rule-description ] ] ]</code>	

### Configure VOICE VLAN Rules

Under the port where port security function has been enabled, if users hope that the terminal accessed can communicate event if it doesn't match the VOICE-VLAN packets of MAC rules and IP rules, and that it is not limited by the number of addresses of MAX rules, they can configure VOICE VLAN rules which will permit all the packets of OUI configured for VOICE-VLAN by OUI to pass.

Table 83 Configuring VOICE VLAN Rules

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2 Ethernet interface
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Configure VOICE VLAN Rules	<b>port-security permit voice vlan</b>	Mandatory  By default, VOICE VLAN rules are not configured under the port.

### Note

- The source MAC permitted by voice vlan rules comes from the OUI configured by

---

VOICE-VLAN.

- After MAX rules are enabled, voice vlan rules will not take effect.
- 

### 83.2.3 Configure STICKY Rules Learning Mode

#### Configuration Condition

Before configuring STICKY rules learning mode, ensure that:

- Enable the port security function.

#### Configure STICKY Rules Learning Mode

If users wish the STICKY rules learning is conducted by MAC or AC+VLAN, the STICKY rules learning mode can be configured as MAC; if users wish the STICKY rules learning is conducted by MAC+IP, the STICKY rules learning mode can be configured as MAC+IP.

Table 83 Configuring STICKY Rules Learning Mode

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected. After you enter the layer-2 Ethernet interface
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Configure STICKY Rules Learning Mode	<b>port-security permit mac-address sticky mode { mac   mac-ip }</b>	Mandatory By default, the STICKY rules learning mode is MAC.

## 83.2.4 Configure Static MAC Address Aging Function

### Configuration Condition

Before configuring the static MAC address aging function, ensure that:

- Enable the port security function.

### Enable Static MAC Address Aging Function

In order to detect whether the terminal corresponding to the valid entries of MAC rules or IP rules is online, the static MAC address aging function can be enabled. After the static MAC address aging function is enabled, if the terminal is checked offline, the valid entries corresponding to this terminal will be deleted so that the chip resources can be released.

Table 6 Enabling Static MAC Address Aging Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected. After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Enable Static MAC Address Aging Function	<b>port-security aging static</b>	Mandatory By default, the static MAC address aging function is closed.

### Configure Static MAC Address Aging Time

Users can configure a reasonable aging time based on the actual network environment. In general applications, keep the default value.

Table 7 Configuring Static MAC Address Aging Time

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Configure Static MAC Address Aging Time	<b>port-security aging time</b> <i>time-value</i>	Mandatory  By default, the static MAC address aging time is 1 minute.

### 83.2.5 Configure Processing Mode After Receiving Illegal Packets

#### Configuration Condition

Before configuring the processing mode when illegal packets are received, ensure that:

- Enable the port security function.

#### Configure Processing Mode After Receiving Illegal Packets

Port security provides three processing modes for illegal packets, i.e. protect, restrict, and shutdown. Users can select them according to their requirements for security. The specific functions of these three processing modes are shown below:

- **Protect:** Discard the illegal packets after receiving them;

- **Restrict:** Discard the packets and trap the information to network management after receiving them;
- **Shutdown:** Discard the packets, close the port which receives them, and trap the information to network management after receiving them.

Table 8 Configuring Processing Mode After Receiving Illegal Packets

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected. After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Configure the processing mode of illegal packets	<b>port-security violation</b> { <b>protect</b>   <b>restrict</b>   <b>shutdown</b> }	Mandatory By default, the processing mode of port security after receiving illegal packets is <b>protect</b> .

### 83.2.6 Configure Log Sending Interval After Receiving Illegal Packets

#### Configuration Condition

Before configuring the log sending interval after receiving illegal packets, ensure that:

- Enable the port security function.

#### Configure Log Sending Interval After Receiving Illegal Packets

Users may configure the log sending interval after receiving illegal packets as needed. In general applications, keep the default value.

Table 9 Configuring Processing Mode After Receiving Illegal Packets

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure Log Sending Interval After Receiving Illegal Packets	<b>port-security violation log-interval</b> <i>log-interval-value</i>	Mandatory By default, the log sending interval is 5 seconds when the port security receives illegal packets.

### 83.2.7 Configure Port Security to Use ACL Function

#### Configuration Condition

Before configuring port security to use ACL function, do the following:

- Enable the port security function.

#### Configure Port Security to Use ACL Function

Users may configure port security to use ACL or not as needed. When using ACL, MAC+IP, MAC+IPv6, STICKY MAC+IP, and STICKY MAC+IPv6 rules can accurately match users' source MAC address and source IP/IPv6 address to prevent the illegal users with matched source MAC address and unmatched source IP/IPv6 address from accessing.

Table 10 Configuring Processing Mode After Receiving Illegal Packets

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent

Step	Command	Description
		configuration takes effect only within the aggregation group.
Configure port security to use ACL function	<b>port-security use-acl</b>	Mandatory By default, port security doesn't use ACL.

### 83.2.8 Port Security Monitoring and Maintaining

Table 11 Port Security Monitoring and Maintaining

Command	Description
<b>clear port-security statistics</b>	Clear statistics of sending and receiving packets
<b>show port-security</b>	Show port summary with port security configuration
<b>show port-security ip-address</b>	Show the IP rules configured
<b>show port-security ipv6-address</b>	Show the IPv6 rules configured
<b>show port-security mac-address</b>	Show the MAC rules and STICKY rules configured
<b>show port-security active-address</b>	Show the information of all valid entries
<b>show port-security detect-mac</b>	Show the new MAC entries currently detected
<b>show port-security violation log-interval</b>	Show the log printing cycle when any illegal MAC entry is detected
<b>show port-security violation-mac</b>	Show the illegal MAC entries currently detected
<b>show port-security statistics</b>	Show statistics of sending and receiving packets

## 83.3 Typical Configuration Example of Port Security

### 83.3.1 Configure MAC and IP Rules for Port Security

#### Network Requirements

- PC1, PC2 and network printer access the server through the Device.
- Configure port security function on the Device. Allow PC1 to pass, reject PC2, and permit the network printer to perform the printing task assigned by the server and PC1 users.

#### Network Topology

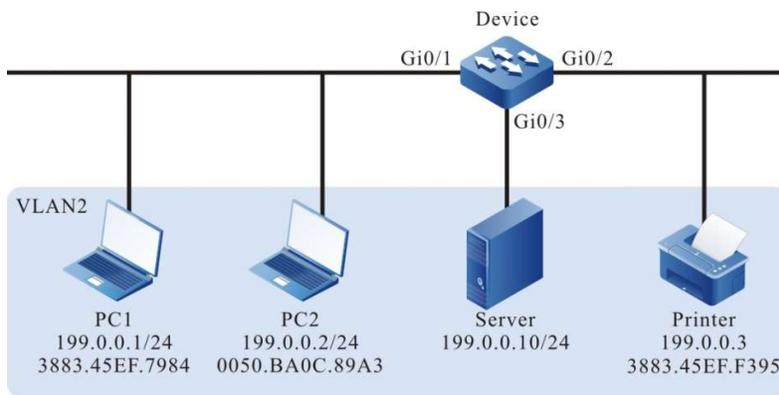


Figure 83 Network Topology for Configuring MAC and IP Rules for Port Security

#### Configuration Steps

Step 1: Configure VLAN.

#Create VLAN 2.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the link type of ports gigabitethernet0/1~gigabitethernet0/3 on the Device as Access, allowing the services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/1-0/3
Device(config-if-range)#switchport mode access
Device(config-if-range)#switchport access vlan 2
Device(config-if-range)#exit
```

Step 2: Configure the port security function.

#Configure MAC+IP rules on gigabitethernet0/1 of the Device to permit PC1 to pass, and configure IP rules to reject PC2.

```

Device#config terminal
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#port-security enable
Device(config-if-gigabitethernet0/1)#port-security permit mac-address 3883.45ef.7984 ip-address 199.0.0.1
Device(config-if-gigabitethernet0/1)#port-security deny ip-address 199.0.0.2
Device(config-if-gigabitethernet0/1)#exit

```

#Configure MAC rules on gigabitethernet0/2 of the Device, permitting the network printer to access the network.

```

Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#port-security enable
Device(config-if-gigabitethernet0/2)#port-security permit mac-address 3883.45ef.f395
Device(config-if-gigabitethernet0/2)#exit

```

Step 3: Check the result.

#View valid entries of port security on the Device. It is indicated that the MAC of PC1 and network printer has been written into the valid entries of port security.

```

Device#show port-security active-address
-----
Entry Interface      MAC address      VID IP/IPv6 Addr  Derivation  Age(Sec)
-----
1   gi0/1             38:83:45:EF:79:84 2   199.0.0.1      MAC+HP      0
2   gi0/2             38:83:45:EF:F3:95 2   199.0.0.3      MAC         0

```

#Through verification, it is indicated that PC1 can access the server and the network printer can perform the printing task assigned by PC1 and the server.

#Through verification, it is indicated that PC2 cannot ping the server and network printer.

### 83.3.2 Configure MAX Rules for Port Security

#### Network Requirements

- PC1, PC2, and PC3 simultaneously access the server through the Device. The PC and the server are in the same LAN.
- Configure port security rules on the Device to permit PC1 and PC2 instead of PC3 to access the server.

#### Network Topology

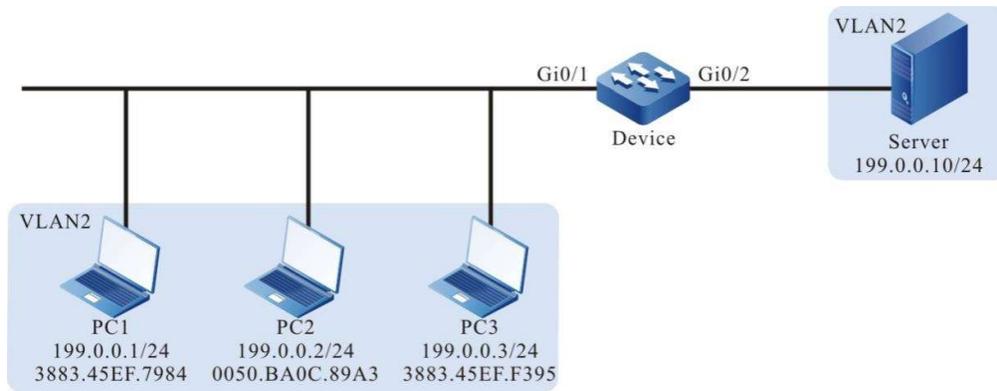


Figure 83 Network Topology for Configuring MAC Rules for Port Security

### Configuration Steps

Step 1: Configure VLAN.

#Create VLAN 2.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the link type of ports gigabitethernet0/1~gigabitethernet0/2 on the Device as Access, allowing the services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/1-0/2
Device(config-if-range)#switchport mode access
Device(config-if-range)#switchport access vlan 2
Device(config-if-range)#exit
```

Step 2: Configure port security rules on the Device.

#Configure MAX rules on gigabitethernet0/1 of the Device, 3 at most.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#port-security enable
Device(config-if-gigabitethernet0/1)#port-security maximum 3
Device(config-if-gigabitethernet0/1)#exit
```

#Reject PC3 to access the server on giabitethernet0/1 of the Device.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#port-security deny mac-address 3883.45ef.f395
Device(config-if-gigabitethernet0/1)#exit
```

Step 3: Check the result.

#Three PCs try to communicate with the server. It is indicated that PC1 and PC2 can access the server, but PC3 cannot do so. #View valid entries of port security on gigabitethernet0/1 of the Device. It is indicated that the MAC addresses of PC1 and PC2 have been written into the valid entries of port security.

```
Device#show port-security active-address
```

Entry	Interface	MAC address	VID	IP/IPv6 Addr	Derivation	Age(Sec)
1	gi0/1	00:50:ba:0c:89:a3	2	---	FREE	0
2	gi0/1	38:83:45:EF:79:84	2	---	FREE	0

Total Mac Addresses for this criterion: 2

### 83.3.3 Configure STICKY Rules for Port Security

#### Network Requirements

- PC1, PC2, and PC3 access the server through the Device. The PC and the server are in the same LAN.
- Configure port security rules on the Device, permitting two PCs to pass.
- After saving the configuration and restarting the Device, the STICKY rules before restarting can take effect immediately.

#### Network Topology

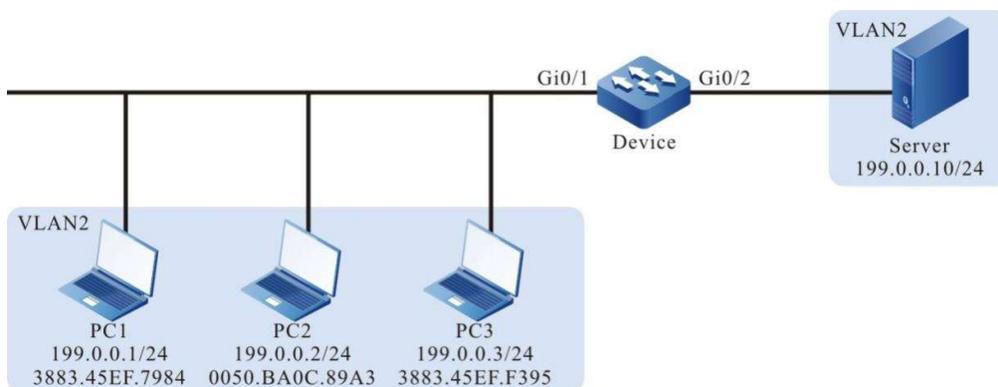


Figure 1 Network Topology for Configuring STICKY Rules for Port Security

#### Configuration Steps

Step 1: Configure VLAN.

#Create VLAN 2.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the link type of ports gigabitethernet0/1~gigabitethernet0/2 on the Device as Access, allowing the services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/1-0/2
Device(config-if-range)#switchport mode access
Device(config-if-range)#switchport access vlan 2
Device(config-if-range)#exit
```

Step 2: Configure MAX rules for port security on the Device.

#Configure MAX rules on gigabitethernet0/1 of the Device, 2 at most.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#port-security enable
Device(config-if-gigabitethernet0/1)#port-security maximum 2
Device(config-if-gigabitethernet0/1)#exit
```

Step 3: Configure STICKY rules for port security on the Device.

#On gigabitethernet0/1 of the Device, enable the STICKY function.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#port-security permit mac-address sticky
Device(config-if-gigabitethernet0/1)#exit
```

Step 4: #Check the configuration result.

#PC1, PC2 and PC3 try to communicate with the server. By checking the valid entries of port security on gigabitethernet0/1 of the Device, it is indicated that the rules on gigabitethernet0/1 are STICKY rules.

```
Device#show port-security active-address
-----
Entry Interface      MAC address      VID IP/IPv6 Addr  Derivation  Age(Sec)
-----
1   gi0/1             38:83:45:EF:79:84 2  199.0.0.1        STICKY      0
2   gi0/1             38:83:45:EF:F3:95 2  199.0.0.3        STICKY      0
Total Mac Addresses for this criterion: 2
```

#After saving the configuration and restarting the Device, the STICKY rules before restarting exist and take effect.

```
Device#show port-security active-address
-----
Entry Interface      MAC address      VID IP/IPv6 Addr  Derivation  Age(Sec)
-----
1   gi0/1             38:83:45:EF:79:84 2  199.0.0.1        STICKY      0
2   gi0/1             38:83:45:EF:F3:95 2  199.0.0.3        STICKY      0
Total Mac Addresses for this criterion: 2
```

# 84 IP Source Guard

---

## 84.1 Overview

IP Source Guard is a packet filtering function. It can filter and control the packets forwarded by the port to prevent illegal packets from passing through the port and improve the security of the port. This function has two types:

1. Port IP Source Guard, i.e. filter the IP packets received by the specified port. The filtering methods include IP, MAC, and IP+MAC. For the specific processing method, see the content below:

- IP: If the source IP address and VLAN ID in the packets are the same as the IP address and VLAN ID recorded in the binding entries, the port will forward the packets; otherwise, it will discard them;
- MAC: If the source MAC address in the packets is the same as the MAC address and VLAN ID recorded in the binding entries, the port will forward the packets; otherwise, it will discard them;
- IP+MAC: If the source IP address, source MAC address and VLAN ID in the packets are the same as the IP address, MAC address and VLAN ID recorded in the binding entries, the port will forward the packets; otherwise, it will discard them.
- The setting of filtration type is valid for dynamic binding entries instead of static ones.
- The binding entries of port IP Source Guard have two types:
- Static binding entries, manually configured static binding entries of port IP Source Guard;
- Dynamic binding entries, dynamically generated by the valid entries of DHCP Snooping function.

2. Global IP Source Guard, i.e. filter the packets received by all the ports, including ARP (Address Resolution Protocol) and IP packets. The filtering methods are shown below:

- If the source IP address in the IP packets is the same as the IP address in the binding entries of global IP Source Guard yet the source MAC address is different, and the source MAC address in the IP packets is the same as the MAC address in the binding entries of global IP Source Guard yet the source IP address is different, the packets will be discarded;

- If the IP address of sending end in the ARP packets is the same as the IP address in the binding entries yet the source MAC address is different, the source MAC address in the ARP packets is the same as the MAC address in the binding entries yet the IP address of sending end is different, the packets will be discarded.

## 84.2 IP Source Guard Function Configuration

Table 84 IP Source Guard Function Configuration List

Configuration Task	
Configure static binding entries for port IP Source Guard	Configure static binding entries for port IP Source Guard
Configure the port IP Source Guard function	Configure the port IP Source Guard function
	Configure port IP Source Guard to filter packet type
Configure global IP Source Guard function	Configure global IP Source Guard function

### 84.2.1 Configure Static Binding Entries for Port IP Source Guard

#### Configuration Condition

Before configuring the static binding entries for port IP Source Guard, do the following:

- Enable the port IP Source Guard function or port Dynamic ARP Inspection function.

#### Configure Static Binding Entries for Port IP Source Guard

The static binding entries of port IP Source Guard serve as the basis of filtering the IP packets received by the specified port.

When the port Dynamic ARP Inspection function is enabled, the static binding entries of the port IP Source Guard can serve as the basis of checking the legality of ARP packets only when the static entries of mac, ip and vlan are configured.

Table 84 Configure Static Binding Entries for Port IP Source Guard

Step	Command	Description
Enter the global configuration mode.	<b>config terminal</b>	-

Step	Command	Description
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Configure static binding entries for port IP Source Guard	<b>ip source binding</b> { <b>ip-address</b> <i>ip-address</i> [ <b>mac-address</b> <i>mac-address</i> [ <b>vlan</b> <i>vlan-id</i> ]   <b>vlan</b> <i>vlan-id</i> ]   <b>mac-address</b> <i>mac-address</i> [ <b>vlan</b> <i>vlan-id</i> ] }	Mandatory  By default, there are no static binding entries of port IP Source Guard.

---

## Note

- For the port Dynamic ARP Inspection function, see the Dynamic ARP Inspection-related chapter in the User Manual.
- 

## 84.2.2 Configure the Port IP Source Guard Function

### Configuration Condition

None

### Configure the Port IP Source Guard Function

After the port IP Source Guard function is enabled, first write the binding entries of port into the chip, including static binding entries with a higher priority and dynamic binding entries. Then, control security of the IP packets received by the port according to the entries written into the chip to prove security.

Table 1 Configure Port IP Source Guard Function

Step	Command	Description
Enter the global configuration mode.	<b>config terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Enable the port IP Source Guard function	<b>ip verify source</b>	Mandatory  By default, the port IP Source Guard function is disabled.

## Note

- After the port IP Source Guard function is enabled, the binding entries of port IP Source Guard are written into the chip, the number of which depends on the available sources of chip entries. If the sources of chip entries are not available, and it's necessary to add binding entries or enable the port IP Source Guard function on other ports, then the binding entries related to the sources of chip entries need to be deleted.
- If some binding entries of the port IP Source Guard fail to be written into the chip due to inadequate sources of chip entries, the system will automatically try to rewrite these binding entries into the chip every 60 seconds until all the binding entries that fail to be written into the chip are written into the chip or deleted.
- If both port IP Source Guard and global IP Source Guard are enabled, the IP packets received by the port can be forwarded only when they match the binding entries of port IP Source Guard and global IP Source Guard; otherwise, they will be discarded.
- Before enabling the port IP Source Guard function, if the terminal device connected to this port is a non-DHCP (Dynamic Host Configuration) client, or if the terminal device is a DHCP client, but it doesn't enable the DHCP Snooping function, the MAC address, IP address and corresponding VLAN number of the terminal device need to be configured as the static binding entries of port IP Source Guard to ensure that after this function is enabled, the

---

terminal device can normally communicate. For the DHCP Snooping function, refer to the DHCP Snooping-related chapters in the User Manual.

---

### 84.2.3 Configure Port IP Source Guard to Filter Packet Type

#### Configuration Condition

Before configuring the port IP Source Guard to filter packet type, do the following:

- Enable the port IP Source Guard function

#### Configure Port IP Source Guard to Filter Packet Type

After enabling the port IP Source Guard function, filter the IP packets in ip mode. When the source IP address and VLAN number in the IPv4 packets received by the port are both the same as those in the binding entries of port IP Source Guard, this port will forward these packets; otherwise, it will discard them.

After the IP Source Guard function of the port is enabled, filter the IP packets in ip-mac mode. When the source MAC address, source IP address and VLAN number in the IP packets received by the port are all the same as the MAC address, IP address and VLAN number in the binding entries of port IP Source Guard, the port will forward these packets; otherwise, it will discard them.

After enabling the IP Source Guard function of the port, filter the IP packets in mac mode. When the source MAC address and VLAN number in the IP packets received by the port are both the same as the MAC address and VLAN number in the binding entries of port IP Source Guard, this port will forward these packets; otherwise, it will discard them.

Table 2 Configuring Port IP Source Guard to Filter Packet Type

Step	Command	Description
Enter the global configuration mode.	<b>config terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected. After you enter the layer-2 Ethernet interface
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect

Step	Command	Description
		only within the aggregation group.
Configure port IP Source Guard to filter packet type	<b>ip verify source type { ip   ip-mac   mac }</b>	Mandatory  By default, the filtering method is ip, which takes effect for dynamic entries only.

## 84.2.4 Configure the Function of Binding Static Entries of Port MAC

### Configuration Condition

#### The Function of Binding Static Entries of Port MAC Is not Configured

After configuring the function of binding static entries of port MAC, corresponding mac address, vlan number and port number are obtained to distribute corresponding static MAC entries from the static entries of IP Source Guard configured and the dynamic entries obtained on the port.

Table 3 Configuring Function of Binding Static MAC Entries

Step	Command	Description
Enter the global configuration mode.	<b>config terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.

Step	Command	Description
Configure the function of binding static entries of port MAC	<b>ip source sticky-mac</b>	Mandatory By default, the function of binding static entries of port MAC is disabled.

## 84.2.5 Configure Global IP Source Guard Function

### Configuration Condition

None

### Configure Global IP Source Guard Function

In order to protect the security of users' IP address and prevent other users from embezzling their IP address, the IP Source Guard function can be configured to bind users' IP address and MAC address. The binding entries of global IP Source Guard of users' IP address and MAC address configured will be directly written into the chip to realize the filtration of illegal IP and ARP packets.

When the global Dynamic ARP Inspection function is enabled, the binding entries of the global IP Source Guard configured can serve as the basis of checking the legality of ARP packets by the global Dynamic ARP Inspection function.

Table 4 Configuring Global IP Source Guard Function

Step	Command	Description
Enter the global configuration mode.	<b>config terminal</b>	-
Configure global IP Source Guard function	<b>source binding mac-address ip-address</b>	Mandatory By default, there are no binding entries of global IP Source Guard. This function is disabled.  This command enables the global IP Source Guard function, and configures a binding entry of global IP Source Guard.

---

## Note

- At most 40 binding entries of global IP Source Guard are supported. The configuration will fail once the number exceeds 40.
  - The binding entries of global IP Source Guard configured are directly written into the chip, the number of which depends on the available sources of chip entries. If the sources of chip entries are not available, and it's necessary to add the binding entries of global IP Source Guard, then the binding entries related to the sources of chip entries need to be deleted.
  - If both port IP Source Guard and global IP Source Guard are enabled, the IP packets received by the port can be forwarded only when they match the binding entries of port IP Source Guard and global IP Source Guard; otherwise, they will be discarded.
- 

---

## Note

- For the global Dynamic ARP Inspection function, see the Dynamic ARP Inspection-related chapter in the User Manual.
- 

## 84.2.6 IP Source Guard Monitoring and Maintaining

Table 84 IP Source Guard Monitoring and Maintenance

Command	Description
<b>show ip binding table</b> [ <b>interface</b> <i>interface-name</i>   <b>link-aggregation</b> <i>link-aggregation-id</i>   <b>slot</b>   <b>summary</b> ]	Show the binding entries of port IP Source Guard and the statistics of the number of binding entries
<b>show ip source guard</b> [ <b>interface</b> { <i>interface-name</i>   <b>link-aggregation</b> <i>link-aggregation-id</i> } ]	Show the configuration of port IP Source Guard function
<b>show source binding</b>	Show the binding entries of global IP Source Guard and the statistics of the number of entries

## 84.3 Typical Configuration Example of IP Source Guard

### 84.3.1 Configure Valid Port IP Source Guard Function Based on Dynamic Entries of DHCP Snooping

#### Snooping

#### Network Requirements

- PC1 and PC2 access IP network through the Device.
- Configure the DHCP Snooping function.
- Configure the port IP Source Guard function so that PC1 instead of PC2 can normally access the IP Network.

#### Network Topology

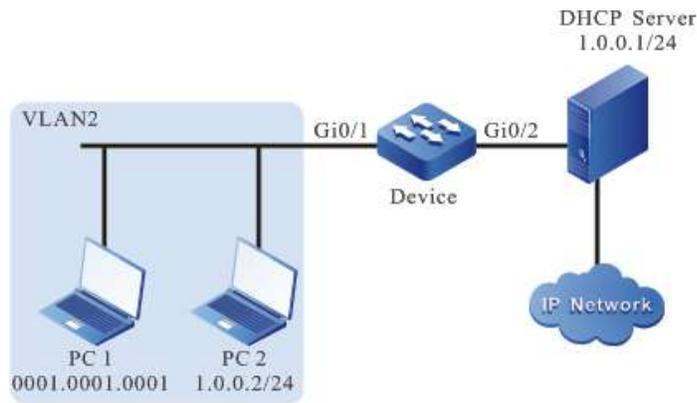


Figure 84-1 Network Topology for Configuring Valid Port IP Source Guard Function Based on Dynamic Entries of DHCP Snooping

#### Configuration Steps

Step 1: Configure VLAN and port link type on Device.

#Create VLAN 2.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the link type of port gigabitethernet0/1 as Access to allow services of VLAN 2 to pass.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode access
Device(config-if-gigabitethernet0/1)#switchport access vlan 2
Device(config-if-gigabitethernet0/1)#exit
```

Step 2: On the Device, enable the global DHCP Snooping function, and configure the gigabitethernet0/2 connected to DHCP Server as a trusted port.

```
Device(config)#dhcp snooping enable
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#dhcp snooping trust
Device(config-if-gigabitethernet0/2)#exit
```

Step 3: Configure the address pool of DHCP Server as 1.0.0.0/24. (omitted)

Step 4: On the Device, configure the port IP Source Guard function.

#On the port gigabitethernet0/1, enable the port IP Source Guard function.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#ip verify source
Device(config-if-gigabitethernet0/1)#exit
```

Step 5: Check the result.

#View DHCP Snooping-related configuration information.

```
Device#show dhcp-snooping
dhcp-snooping configuration information:
dhcp-snooping status:enable
dhcp-snooping option82 information status:disable
dhcp-snooping option82 information policy:replace
dhcp-snooping option82 information format:default
dhcp-snooping option82 information remote id:default(mac address)
dhcp-snooping information relay-address :None
dhcp-snooping binding agent save mode :auto-flash
dhcp-snooping binding agent save delay :1800
dhcp-snooping binding agent save pool :30
dhcp-snooping interface information :
-----
interface      trust-status  rate-limit(pps)  circuit-Id
gi0/0/1        untrust      40                default(vlan-mod-interface)
gi0/0/2        trust        ----              default(vlan-mod-interface)
gi0/0/3        untrust      40                default(vlan-mod-interface)
gi0/0/4        untrust      40                default(vlan-mod-interface)
gi0/0/5        untrust      40                default(vlan-mod-interface)
.....
```

#View IP Source Guard-related configuration information.

```
Device#show ip source guard
-----
IP source guard interfaces on slot 0 :
    Total number of enabled interfaces : 1
-----
Interface Name      Status   Verify Type  L2 Status
-----
gi0/1               Enabled  ip           Disabled
gi0/2               Disabled ip           Disabled
gi0/3               Disabled ip           Disabled
gi0/4               Disabled ip           Disabled
gi0/5               Disabled ip           Disabled
.....
```

It is indicated that the port gigabitethernet0/1 has enabled the IP Source Guard function, and the Verify Type is ip. Therefore, in the example mentioned above, dynamic entries will take effect based on ip+vlan.

#View the binding entries of port IP Source Guard.

```
Device#show ip binding table
-----
IP Source Guard binding table on slot 0
    Total binding entries   : 1
    Static binding entries  : 0
    Dynamic binding entries  : 1
    Dynamic not write entries : 0
    PCE writing entries      : 1
-----
Interface-Name  MAC-Address  IP-Address  VLAN-ID  Type-Flag  Writing-Flag  L2-Flag
-----
gi0/1           0001.0001.0001  1.0.0.2    2        dynamic    Write         Not Write
```

#PC1 instead of PC2 can normally access the IP Network.

### 84.3.2 Configure the Port IP Source Guard Function Which Takes Effect Based on Static Entries

#### Network Requirements

- PC1 and PC2 access IP network through the Device.
- Configure the port IP Source Guard function which takes effect based on static entries

so that PC1 instead of PC2 can normally access the IP Network.

## Network Topology

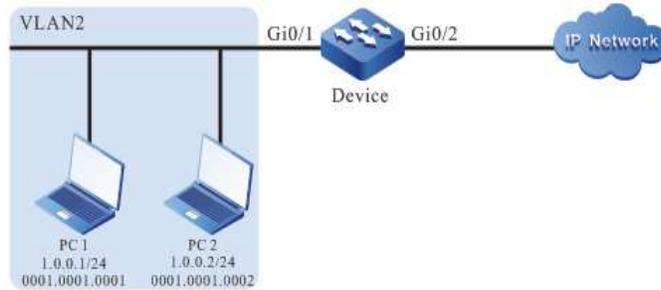


Figure 84-2 Network Topology for Configuring Valid Port IP Source Guard Function Based on Static Entries

## Configuration Steps

Step 1: Configure VLAN and port link type on Device.

#Create VLAN 2.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the link type of port gigabitethernet0/1 as Access to allow services of VLAN 2 to pass.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode access
Device(config-if-gigabitethernet0/1)#switchport access vlan 2
Device(config-if-gigabitethernet0/1)#exit
```

Step 2: On the Device, configure the port IP Source Guard function.

#Enable the port IP Source Guard function based on MAC+VLAN filtering method on port gigabitethernet0/1, and configure the binding entries of port IP Source Guard with IP address of 1.0.0.1 and VLAN 2.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#ip verify source
Device(config-if-gigabitethernet0/1)#ip source binding ip-address 1.0.0.1 vlan 2
Device(config-if-gigabitethernet0/1)#exit
```

Step 3: Check the result.

#View IP Source Guard-related configuration information.

```
Device#show ip source guard
-----
IP source guard interfaces on slot 0 :
```

Total number of enabled interfaces : 1

Interface Name	Status	Verify Type	L2 Status
gi0/1	Enabled	IP	Disabled
gi0/2	Disabled	IP	Disabled
gi0/3	Disabled	IP	Disabled
gi0/4	Disabled	IP	Disabled
.....			

It is indicated that the port gigabitethernet0/1 has enabled the IP Source Guard function. The static IP Source Guard entries that take effect according to the IP+VLAN entries configured have nothing to do with Verify Type value. Therefore, the example mentioned above takes effect based on IP+VLAN.

#View the binding entries of port IP Source Guard.

```
Device #show ip binding table
-----
IP Source Guard binding table on slot 0
  Total binding entries   : 1
  Static binding entries  : 1
  Dynamic binding entries : 0
  Dynamic not write entries : 0
  PCE writing entries     : 1
-----
Interface-Name  MAC-Address  IP-Address  VLAN-ID  Type-Flag  Writing-Flag  L2-Flag
-----
gi0/1          ---          1.0.0.1    2        Static    Write        Not Write
```

#PC1 instead of PC2 can normally access the IP Network.

# 85 IPv6 Source Guard

---

## 85.1 Overview

IPv6 Source Guard is a packet filtering function. It can filter and control the packets forwarded by the port to prevent illegal packets from passing through the port and improve the security of the port. This function has two types:

1. Port IPv6 Source Guard, i.e. filter the IPv6 packets received by the specified port. The filtering methods include IP, IP+MAC and MAC. For the specific processing method, see the content below:

- IP: If the source IPv6 address and VLAN ID in the packets are the same as the IPv6 address and VLAN ID recorded in the binding entries, the port will forward the packets; otherwise, it will discard them;
- IP+MAC+VLAN: If the source IPv6 address, source MAC address and VLAN ID in the packets are the same as the IPv6 address, MAC address and VLAN ID recorded in the binding entries, the port will forward the packets; otherwise, it will discard them.
- MAC+VLAN: If the source MAC address and VLAN ID in the packets are the same as the MAC address and VLAN ID recorded in the binding entries, the port will forward the packets; otherwise, it will discard them.
- The setting of filtration type is valid for dynamic binding entries instead of static ones.

The binding entries of port IPv6 Source Guard have two types:

- Static binding entries, manually configured static binding entries of port IPv6 Source Guard;
- Dynamic binding entries, dynamically generated by the valid entries of DHCPv6 Snooping function.

2. Global IPv6 Source Guard, i.e. filter the packets received by all the ports. The filtering methods are shown below:

- If the source IPv6 address and MAC address in IPv6 packets are different from any one of the IPv6 address and source MAC address in the binding entries of global IPv6 Source Guard, the packets will be discarded.

## 85.2 IPv6 Source Guard Function Configuration

Table 85 IPv6 Source Guard Function Configuration List

Configuration Task	
Configure Basic Functions of Port IPv6 Source Guard	Enable Port IPv6 Source Guard Function
	Configure Number of Binding Entries of Port IPv6 Source Guard
Configure Port IPv6 Source Guard to Filter Packet Type	Configure Port IPv6 Source Guard to Filter Packet Type
Configuring Static Binding Entries for Port IPv6 Source Guard	Configuring Static Binding Entries for Port IPv6 Source Guard
Configure the function of binding static entries of port MAC	Configure the function of binding static entries of port MAC
Configure Global IPv6 Source Guard Function	Configure Global IPv6 Source Guard Function

### 85.2.1 Enable Port IPv6 Source Guard Function

#### Configuration Condition

- None

#### Enable Port IPv6 Source Guard Function

After the port IPv6 Source Guard function is enabled, the binding entries (static and dynamic entries) on the port will be written into the hardware. Only the packets that completely match the characteristics of the binding entries can be forwarded. Others will be discarded. This can achieve the purpose of security protection. After IPv6 Source Guard is enabled, the DHCPv6 packets and ND packets under this port are permitted to pass by default.

Table 85 Enabling Port IPv6 Source Guard Function

Step	Command	Description
Enter the global configuration mode.	<b>config terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration

Step	Command	Description
		takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enable Port IPv6 Source Guard Function	<b>ipv6 verify source</b>	Mandatory  By default, the IPv6 Source Guard function is disabled on the port.

## 85.2.2 Configure Number of Binding Entries of Port IPv6 Source Guard

### Configuration Condition

Before configuring the number of binding entries for port IPv6 Source Guard, do the following:

- Enable port IPv6 Source Guard function.

### Configure Number of Binding Entries of Port IPv6 Source Guard

The upper limit of the number of binding entries (including static and dynamic binding entries) supported by the port, to prevent a single port from being attached and occupying device resources.

Table 1 Configuring Number of Binding Entries of Port IPv6 Source Guard

Step	Command	Description
Enter the global configuration mode.	<b>config terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	

Step	Command	Description
		configuration takes effect only within the aggregation group.
Configure Number of Binding Entries of Port IPv6 Source Guard	<b>ipv6 verify source max-entries</b> <i>number</i>	Mandatory  By default, 536 binding entries can be configured for each port.

### 85.2.3 Configure Port IPv6 Source Guard to Filter Packet Type

#### Configuration Condition

Before configuring the port IPv6 Source Guard to filter packet type, do the following:

- Enable port IPv6 Source Guard function.

#### Configure Port IPv6 Source Guard to Filter Packet Type

After enabling the port IPv6 Source Guard function, filter the IPv6 packets in ip mode. When the source IPv6 address and VLAN number in the IPv6 packets received by the port are both the same as those in the binding entries of port IPv6 Source Guard, this port will forward these packets; otherwise, it will discard them.

After the port IPv6 Source Guard function is enabled, filter the IPv6 packets in ip-mac mode. When the source MAC address, source IPv6 address and VLAN number in the IPv6 packets received by the port are all the same as the MAC address, IPv6 address and VLAN number in the binding entries of port IPv6 Source Guard, the port will forward these packets; otherwise, it will discard them.

After enabling the port IPv6 Source Guard function, filter the IPv6 packets in mac mode. When the source MAC address and VLAN number in the IPv6 packets received by the port are both the same as the MAC address and VLAN number in the binding entries of port IPv6 Source Guard, this port will forward these packets; otherwise, it will discard them.

Table 2 Configure Port IPv6 Source Guard to Filter Packet Type

Step	Command	Description
Enter the global configuration mode.	<b>config terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.

Step	Command	Description
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Configure Port IPv6 Source Guard to Filter Packet Type	<b>ipv6 verify source type {ip   ip-mac   mac}</b>	Mandatory  By default, the port filters packets in ip-only mode.

---

### Note

- After the port IPv6 Source Guard function is enabled, the binding entries of port IPv6 Source Guard are written into the chip, the number of which depends on the available sources of chip entries. If the sources of chip entries are not available, and it's necessary to add binding entries or enable the port IPv6 Source Guard function on other ports, then the binding entries related to the sources of chip entries need to be deleted.
  - If some binding entries of the port IPv6 Source Guard fail to be written into the chip due to inadequate sources of chip entries, the system will automatically try to rewrite these binding entries into the chip every 60 seconds until all the binding entries that fail to be written into the chip are written into the chip or deleted.
  - Configure port IPv6 Source Guard to filter packet type and make it take effect for the dynamic entries generated by DHCPv6 Snooping only
- 

## 85.2.4 Configuring Static Binding Entries for Port IPv6 Source Guard

### Configuration Condition

Before configuring static binding entries for port IPv6 Source Guard, do the following:

- Enable port IPv6 Source Guard function.

### Configure Static Binding Entries for Port IP Source Guard

The static binding entries of port IPv6 Source Guard serve as the basis of filtering the IPv6 packets received by the specified port.

Table 85 Configuring Static Binding Entries of Port IPv6 Source Guard Function

Step	Command	Description
Enter the global configuration mode.	<b>config terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Configuring Static Binding Entries for Port IPv6 Source Guard	<b>ipv6 source binding</b> { <b>ipv6-address</b> <i>ipv6-address</i> [ <b>mac-address</b> <i>mac-address</i> [ <b>vlan</b> <i>vlan-id</i> ]   <b>vlan</b> <i>vlan-id</i> ]   <b>mac-address</b> <i>mac-address</i> [ <b>vlan</b> <i>vlan-id</i> ] }	Mandatory  By default, there are no static binding entries of port IPv6 Source Guard.

### 85.2.5 Configure the Function of Binding Static Entries of Port MAC

#### Configuration Condition

The function of binding static entries of port MAC is not configured

After configuring the function of binding static entries of port MAC, corresponding mac address, vlan number and port number are obtained to distribute corresponding static MAC entries from the static entries of IPv6 Source Guard configured and the dynamic entries obtained on the port.

Table 3 Configure Function of Binding Static MAC Entries

Step	Command	Description
Enter the global configuration mode.	<b>config terminal</b>	-

Step	Command	Description
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Configure the function of binding static entries of port MAC	<b>ipv6 source sticky-mac</b>	Mandatory  By default, the function of binding static entries of port MAC is disabled.

## 85.2.6 Configure Global IPv6 Source Guard Function

### Configuration Condition

None

### Configure Global IPv6 Source Guard Function

In order to protect the security of users' IPv6 address and prevent other users from embezzling their own IPv6 address, you can configure the global IPv6 Source Guard function to bind users' IPv6 address and MAC address. The binding entries of global IPv6 Source Guard of users' IPv6 address and MAC address configured will be directly written into the chip to realize the filtration of illegal IPv6 packets.

Table 85 Configuring Global IPv6 Source Guard Function

Step	Command	Description
Enter the global configuration mode.	<b>config terminal</b>	-

Step	Command	Description
Configure Global IPv6 Source Guard Function	<b>ipv6 source binding mac-address <i>mac-address</i> ipv6-address <i>ipv6_address</i></b>	Mandatory  By default, there are no binding entries of global IPv6 Source Guard. This function is disabled.

## Note

- At most 40 binding entries of global IPv6 Source Guard are supported. The configuration will fail once the number exceeds 40.
- The binding entries of global IPv6 Source Guard configured are directly written into the chip, the number of which depends on the available sources of chip entries. If the sources of chip entries are not available, and it's necessary to add the binding entries of global IPv6 Source Guard, then the binding entries related to the sources of chip entries need to be deleted.
- If both port IPv6 Source Guard and global IPv6 Source Guard are enabled, the IPv6 packets received by the port can be forwarded only when they match the binding entries of port IPv6 Source Guard and global IPv6 Source Guard; otherwise, they will be discarded.

## 85.2.7 IPv6 Source Guard Monitoring and Maintaining

Table 4 IPv6 Source Guard Monitoring and Maintenance

Command	Description
<b>show ipv6 binding table [ dynamic   static   interface <i>interface-name</i>   slot   summary ]</b>	Show the binding entries of port IPv6 Source Guard and the statistics of the number of binding entries
<b>show ipv6 source guard [ interface <i>interface-name</i>]</b>	Show the configuration of port IPv6 Source Guard function

## 85.3 Typical Configuration Example of IPv6 Source Guard

### 85.3.1 Configure Valid Port IPv6 Source Guard Function Based on Dynamic Entries of DHCPv6 Snooping

#### Network Requirements

- PC1 and PC2 access IPv6 network through the Device.

- Configure the global DHCPv6 Snooping function.
- Configure the port IPv6 Source Guard function so that PC1 instead of PC2 can normally access the IPv6 Network.

## Network Topology

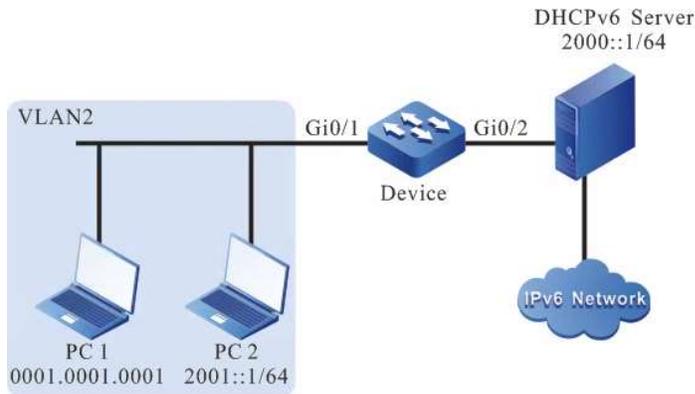


Figure 85 Network Topology for Configuring Valid Port IPv6 Source Guard Function Based on Dynamic Entries of DHCPv6 Snooping

## Configuration Steps

Step 1: Configure VLAN and port link type on Device.

#Create VLAN 2.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the link type of port gigabitethernet0/1 as Access to allow services of VLAN 2 to pass.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode access
Device(config-if-gigabitethernet0/1)#switchport access vlan 2
Device(config-if-gigabitethernet0/1)#exit
```

Step 2: On the Device, enable the global DHCPv6 Snooping function, and configure the gigabitethernet0/2 connected to DHCPv6 Server as a trusted port.

```
Device(config)#ipv6 dhcp snooping enable
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#ipv6 dhcp snooping trust
Device(config-if-gigabitethernet0/2)#exit
```

Step 3: Configure the address pool of DHCPv6 Server as 2000::2/64. (omitted)

Step 4: Configure port IPv6 Source Guard function on the Device.

#On the port gigabitethernet0/1, enable the port IPv6 Source Guard function.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#ipv6 verify source
Device(config-if-gigabitethernet0/1)#exit
```

Step 5: Check the result.

#View DHCPV6 Snooping-related configuration information.

```
Device#show ipv6 dhcp snooping
dhcpv6-snooping configuration information:
dhcpv6-snooping status:enable
dhcpv6-snooping entry aged time:300
dhcpv6-snooping binding agent save delay time:1800
dhcpv6-snooping binding agent save type :FLASH
dhcpv6-snooping binding agent save file :dhcpv6sp_binding.db
dhcpv6-snooping binding agent save pool time:30
dhcpv6-snooping interface information :
-----
interface      trust-status  max-learning-num option-policy  option18-status  option37-status
gi0/1          untrust      1024          keep          disable          disable
      gi0/2          trust        1024          keep          disable          disable
gi0/3          untrust      1024          keep          disable          disable
gi0/4          untrust      1024          keep          disable          disable
gi0/5          untrust      1024          keep          disable          disable
.....
```

#View IPv6 Source Guard-related configuration information.

```
Device#show ipv6 source guard
-----
IPv6 source guard interfaces on slot 0 :
  Total number of enabled interfaces : 1
-----
Interface Name      Status      Verify Type  L2 Status  Max Entry
-----
gi0/1               Enabled     ip           Disabled   536
gi0/2               Disabled    ip           Disabled   536
gi0/3               Disabled    ip           Disabled   536
gi0/4               Disabled    ip           Disabled   536
gi0/5               Disabled    ip           Disabled   536
.....
```

It is indicated that the port gigabitethernet0/1 has enabled the IPv6 Source Guard function, and the Verify Type is ip. Therefore, in the example mentioned above, dynamic entries will take effect based on ip+vlan.

#View the binding entries of port IPv6 Source Guard.

```
Device#show ipv6 binding table
-----global Ipv6 and mac binding entry -----
total :0
-----
IPv6 Source Guard binding table on slot 0
Total binding entries   : 1
Static binding entries  : 0
Static not write entries : 0
Dynamic binding entries : 1
Dynamic not write entries : 0
PCE writing entries     : 1
-----
```

Interface-Name	MAC-Address	VLAN-ID	Type-Flag	Writing-Flag	L2-Flag	IP-Address
gi0/1	0001.0001.0001	2	dynamic	Write	Not Write	2000::2

#PC1 instead of PC2 can normally access the IPv6 Network.

## 85.3.2 Configure the Port IPv6 Source Guard Function Which Takes Effect Based on Static Entries

### Network Requirements

- PC1 and PC2 access IPv6 network through the Device.
- Configure the port IPv6 Source Guard function which takes effect based on static entries so that PC1 instead of PC2 can normally access the IPv6 Network.

### Network Topology

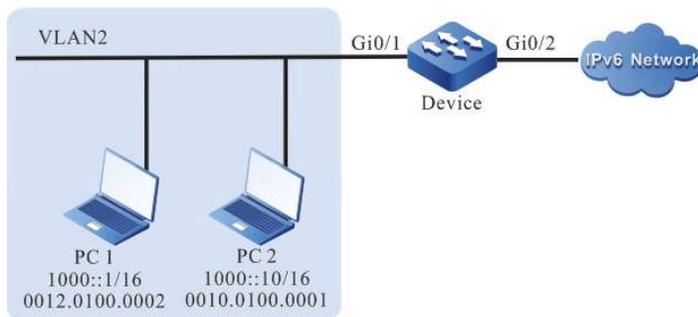


Figure 1 Network Topology for Configuring Valid Port IPv6 Source Guard Function Based on Static Entries

### Configuration Steps

Step 1: Configure VLAN and port link type on Device.

#Create VLAN 2.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the link type of port gigabitethernet0/1 as Access to allow services of VLAN 2 to pass.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode access
Device(config-if-gigabitethernet0/1)#switchport access vlan 2
Device(config-if-gigabitethernet0/1)#exit
```

Step 2: Configure port IPv6 Source Guard function on the Device.

#Enable the port IPv6 Source Guard function based on MAC+VLAN filtering method on port gigabitethernet0/1, and configure the binding entries of port IPv6 Source Guard with IP address of 1000::1 and VLAN 2.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#ipv6 verify source
Device(config-if-gigabitethernet0/1)#ipv6 source binding ipv6-address 1000::1 vlan 2
Device(config-if-gigabitethernet0/1)#exit
```

Step 3: Check the result.

#View IPv6 Source Guard-related configuration information.

```
Device#show ipv6 source guard
-----
IPv6 source guard interfaces on slot 0 :
  Total number of enabled interfaces : 1
-----
Interface Name      Status   Verify Type  L2 Status  Max Entry
-----
gi0/1               Enable   ip           Disabled   536
gi0/2               Disabled ip           Disabled   536
gi0/3               Disabled ip           Disabled   536
gi0/4               Disabled ip           Disabled   536
.....
```

It is indicated that the port gigabitethernet0/1 has enabled the IPv6 Source Guard function. The static IPv6 Source Guard entries that take effect according to the IP+VLAN entries configured have nothing to do with Verify Type value. Therefore, the example mentioned above takes effect based on IP+VLAN.

#View the binding entries of port IPv6 Source Guard.

```
Device #show ipv6 binding table
-----global Ipv6 and mac binding entry -----
total :0
-----

IPv6 Source Guard binding table on slot 0
  Total binding entries   : 1
  Static binding entries  : 1
  Static not write entries : 0
  Dynamic binding entries : 0
  Dynamic not write entries : 0
  PCE writing entries     : 1
-----

Interface-Name  MAC-Address  VLAN-ID  Type-Flag  Writing-Flag  L2-Flag  IP-Address
```

---

gi0/1      ---    2    Static   Write   Not Write   1000::1

#PC1 can normally access the IP Network. PC2 cannot access the IPv6 Network.

# 86 ND Snooping

---

## 86.1 Overview

### ND Snooping

ND Snooping is a security feature of IPv6 ND (Neighbor Discovery), used in layer-2 switching network environment. It builds ND Snooping dynamic binding table by snooping the NS (Neighbor Solicitation) packets of DAD (Duplicate Address Detection) to record the source IPv6 address, source MAC address, VLAN, ingress port, etc. of packets so as to prevent from being attacked by the ND packets of subsequent fake users and gateways.

### Trusted Interface/Untrusted Interface of ND Snooping

Trusted interface of ND Snooping: This type of interface is used to connect trusted IPv6 nodes. The ND packets received from this type of interface will be normally forwarded by the device.

Untrusted interface of ND Snooping: This type of interface is used to connect untrusted IPv6 nodes. For the RA packets and redirected packets received from this type of interface, the device considers them to be illegal and directly discards them; for the NA/NS/RS packets received, if the interface or the VLAN where the interface is located enables the ND packet legality check function, the device will check the binding table matching of NA/NS/RS packets according to the dynamic binding table of ND Snooping. When the packets fail to comply with the binding table relationship, they will be considered as illegal users' packets and directly discarded; for other types of ND packets received, the device forwards them normally.

### ND Snooping binding table

After the ND Snooping function is configured, the device builds a dynamic binding table of ND Snooping by snooping users' NS packets for DAD. The entries include the requested IPv6 address, source MAC address, VLAN and ingress interface in DAD packets. The dynamic binding table of ND Snooping can be used for the device to check the binding table matching of NA/NS/RS packets received from untrusted interface so as to filter illegal NA/NS/RS packets.

## 86.2 ND Snooping Function Configuration

Table 86-1 ND Snooping Function Configuration List

Configuration Task	
Configure Enabling the ND Snooping Function	Configure Enabling the ND Snooping Function

Configuration Task	
Configure Specifying Trusted Interface of ND Snooping	Configure Specifying Trusted Interface of ND Snooping
Configure Static Binding Entries for ND Snooping	Configure Static Binding Entries for ND Snooping
Configure Dynamic Binding Table Detection Function for ND Snooping	Configure Dynamic Binding Table Detection Function for ND Snooping
Configure Enabling ND Snooping Attack Detection Log Function	Configure Enabling ND Snooping Attack Detection Log Function

## 86.2.1 Configure Enabling the ND Snooping Function

### Configuration Condition

None

### Configure Enabling the ND Snooping Function

Table 1 Configuring Enabling ND Snooping Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure to enable the global ND Snooping function	<b>nd snooping enable</b>	Mandatory By default, the global ND Snooping function is disabled.
Enter the layer-2 VLAN configuration mode	<b>vlan <i>vlan-id</i></b>	Mandatory After entering the Layer-2 VLAN configuration mode, subsequent configurations only take effect on current VLAN.
Configure to enable the ND Snooping function under vlan	<b>nd snooping enable</b>	Mandatory By default, the ND Snooping function under VLAN is disabled.

## 86.2.2 Configure Specifying Trusted Interface of ND Snooping

### Configuration Condition

None

### Configure Specifying Trusted Interface of ND Snooping

Table 86-3 Configuring Specifying Trusted Interface of ND Snooping

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure to enable the global ND Snooping function	<b>nd snooping enable</b>	Mandatory By default, the global ND Snooping function is disabled.
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	Mandatory The subsequent configuration takes effect only on the current port after you enter the Layer-2 Ethernet interface configuration mode.
Configure to specify trusted interface	<b>nd snooping trusted</b>	Mandatory By default, the interface is an untrusted interface.

## 86.2.3 Configure Static Binding Entries for ND Snooping

### Configuration Condition

None

### Configure Static Binding Entries for ND Snooping

Table 86-4 Configuring Static Binding Entries of ND Snooping

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure to enable the global ND Snooping function	<b>nd snooping enable</b>	Mandatory By default, the global ND Snooping function is disabled.
Configure Static Binding Entries for ND Snooping	<b>nd snooping user-bind</b> <i>ipv6-address mac-address</i> <b>vlan</b> <i>vlan-id</i> <b>interface</b> <i>interface-name</i>	Optional By default, no static binding entry of ND Snooping is configured.  When there is a static binding entry, match this static binding entry first; when static binding entry is not configured, use dynamic binding entry directly.

#### 86.2.4 Configure Dynamic Binding Table Detection Function for ND Snooping

##### Configuration Condition

None

##### Configure Dynamic Binding Table Detection Function for ND Snooping

Table 86-5 Configuring Dynamic Binding Table Detection Function of ND Snooping

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure to enable the global ND Snooping function	<b>nd snooping enable</b>	Mandatory By default, the global ND Snooping function is disabled.
Configure Dynamic Binding Table Detection Function for ND Snooping	<b>nd snooping detect</b> <b>retransmit</b> <i>retransmits-times</i> <b>interval</b> <i>time</i>	Mandatory By default, the dynamic binding table detection function of ND Snooping is disabled.

## 86.2.5 Configure Enabling ND Snooping Attack Detection Log Function

### Configuration Condition

None

### Configure Enabling ND Snooping Attack Detection Log Function

Table 86-6 Configuring Enabling ND Snooping Attack Detection Log Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure to enable the global ND Snooping function	<b>nd snooping enable</b>	Mandatory By default, the global ND Snooping function is disabled.
Configure Enabling ND Snooping Attack Detection Log Function	<b>nd snooping attack-log enable</b>	Mandatory By default, the ND Snooping attack detection log function is disabled.

## 86.2.6 ND Monitoring and Maintaining

Table 86-7 ND Monitoring and Maintaining

Command	Description
<b>clear nd fast-response statistics</b>	The command is used to clear the ND fast response statistics.
<b>clear nd snooping dynamic-user-bind</b>	The command is used to delete dynamic binding entries of ND Snooping.
<b>clear nd snooping prefix</b>	The command is used to delete prefix entries of ND Snooping.
<b>clear nd snooping statistics</b>	The command is used to clear the statistics of ND Snooping.

Command	Description
<b>show nd fast-response statistics</b>	The command is used to display the ND fast response statistics.
<b>show nd proxy address</b>	The command is used to show nd as the address of external module pickup.
<b>show nd snooping prefix</b>	The command is used to show prefix entries of ND Snooping.
<b>show nd snooping user-bind</b>	The command is used to show binding entries of ND Snooping.
<b>show nd snooping statistics</b>	The command is used to show the statistics of ND Snooping.

## 86.3 Typical Configuration Example of ND Snooping

### 86.3.1 Configure the Basic Functions of ND Snooping

#### Network Requirements

- Device1 connects the gateway device Device2 through gigabitethernet0/3.
- Enable RA service on Device2 (enable RA packet sending function).
- Enable ND Snooping function on Device1. When an attacker sends illegal NS/NA/ RS /RA packets in the network, Device1 will discard these illegal ND packets to guarantee the communication between legal users and gateway.

#### Network Topology

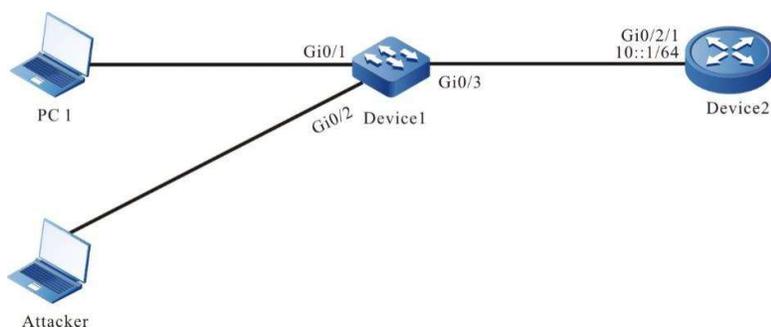


Figure 86 Network Topology for Configuring Basic Functions of ND Snooping

#### Configuration Steps

Step 1: Configure VLAN and port link type on Device1.

#Create VLAN 2.

```
Device1#configure terminal
Device1(config)#vlan 2
Device1(config-vlan2)#exit
```

#Configure the link type of ports gigabitethernet0/1~gigabitethernet0/3 as Access, allowing the services of VLAN2 to pass.

```
Device1(config)#interface gigabitethernet 0/1-0/3
Device1(config-if-range)#switchport mode access
Device1(config-if-range)#switchport access vlan 2
Device1(config-if-range)#exit
```

Step 2: Configure IPv6 address on the layer-3 interface gigabitethernet0/2/1 of the gateway device Device 2.

```
Device2(config)#interface gigabitethernet 0/2/1
Device2 (config-if-gigabitethernet0/2/1)#ipv6 address 10::1/64
Device2 (config-if-gigabitethernet0/2/1)#exit
```

Step 3: Enable RA service on the gateway device Device2 (enable RA packet sending function).

```
Device2(config)#interface gigabitethernet 0/2/1
Device2 (config-if-gigabitethernet0/2/1)#no ipv6 nd suppress-ra period
Device2 (config-if-gigabitethernet0/2/1)#no ipv6 nd suppress-ra response
Device2 (config-if-gigabitethernet0/2/1)#exit
```

Step 4: Configure ND Snooping function on Device1.

#Globally enable the ND Snooping function.

```
Device1(config)#nd snooping enable
```

#Enable ND Snooping function on VLAN 2.

```
Device1(config)#vlan 2
Device1(config-vlan2)#nd snooping enable
Device1(config-vlan2)#exit
```

#Configure the port gigabitethernet0/3 as a trusted interface.

```
Device1(config)#interface gigabitethernet 0/3
Device1(config-if-gigabitethernet0/3)#nd snooping trusted
Device1(config-if-gigabitethernet0/3)#exit
```

Step 5: Check the result.

#View the prefix information obtained by Device1 from the gateway device Device2.

```
Device1#show nd snooping prefix
```

prefix	length	valid-time	preferred-time
10::	64	2592000	604800

```
Total number: 1
```

#After the Ipv6 address 10::3 within the prefix 10::/64 administration scope is configured on PC1, view ND Snooping entries on the Device.

```
Device1#show nd snooping user-bind dynamic
ipv6-address  mac-address  vlan  interface  type
10::3         0857.00da.4715  2    gi0/1      dynamic
```

The ND Snooping entries of the IP, MAC, VLAN, and access port information of PC1 are generated on Device1.

#Attacker simulates the IP of PC1 to send NS, NA and RS packets to the gateway. The Device receives the Attacker's NS, NA, and RS packets, discards them if they are found inconsistent with the recorded ND Snooping entries, and makes relevant records in the statistics of ND Snooping.

```
Device1#show nd snooping statistics
```

Statistics for lpu 0 nd snooping:

```
lladdrInvalid:    0
dadPacketDeal:    0
nsPacketPass:     0
nsPacketDrop:     1
naPacketPass:     0
naPacketDrop:     1
rsPacketDrop:     1
rsPacketPass:     0
raPacketPass:     0
raPacketDrop:     0
rdPacketDrop:     0
rdPacketPass:     0
sendDtPktFail:    0
sendDtPktOk:      0
```

#Attacker simulates the gateway to send RA packets to PC1. The Device receives the Attacker's RA packets, discards them if they are received from an untrusted port, and makes relevant records in the statistics of ND Snooping.

```
Device1#show nd snooping statistics
```

Statistics for lpu 0 nd snooping:

```
lladdrInvalid:    0
dadPacketDeal:    0
nsPacketPass:     0
nsPacketDrop:     0
naPacketPass:     0
naPacketDrop:     0
rsPacketDrop:     0
rsPacketPass:     0
raPacketPass:     0
raPacketDrop:     1
rdPacketDrop:     0
rdPacketPass:     0
sendDtPktFail:    0
sendDtPktOk:      0
```

# 87 DHCP Snooping

---

## 87.1 Overview

### 87.1.1 Basic Functions of DHCP Snooping

DHCP snooping is a security feature of DHCP (Dynamic Host Configuration Protocol). It has the following two functions:

1. Record the corresponding relation between MAC address and IP address of DHCP client:

For the sake of security, the network administrator may need to record the IP address used when users surf the Internet, and confirm the corresponding relation between the MAC address of users' host and the IP address obtained from the DHCP server.

DHCP snooping records the MAC address of DHCP client and the IP address obtained by snooping the DHCP request packets and the DHCP response packets received by the trusted port. The administrator can view the IP address information obtained by the DHCP client through the binding entries recorded by DHCP snooping.

2. Guarantee the client obtains IP address from a legal server:

If there is DHCP server set up in the network without permission, the DHCP client is likely to obtain incorrect IP address, causing abnormal communication or safety hazard. To ensure that the DHCP client can obtain an IP address through a legal DHCP server, the DHCP snooping function permits to configure the port as a trusted port or an untrusted port:

- Trusted port is directly or indirectly connected to a legitimate DHCP server. Trusted port normally forwards the DHCP response packets received so as to ensure that the DHCP client can obtain a correct IP address;
- An untrusted port is not directly or indirectly connected to a legitimate DHCP server. If a DHCP response packet sent by the DHCP server is received from an untrusted port, it will be discarded to prevent the DHCP client from obtaining incorrect IP address.

### 87.1.2 DHCP Snooping Option82

DHCP snooping supports the addition, forwarding and management of Option82. Option82 is a DHCP packet option used to record the location of DHCP client. The administrator can locate DHCP client according to this option for security control, e.g. limit the number of IP addresses that can be assigned by a port or VLAN. Depending on the type of DHCP packets, Option82 can be processed by the following ways:

1. When the device receives a DHCP request packet, it will process the packet according to whether it contains Option82, the processing policy and fill format configured by the user, and forward the processed packet to the DHCP server;

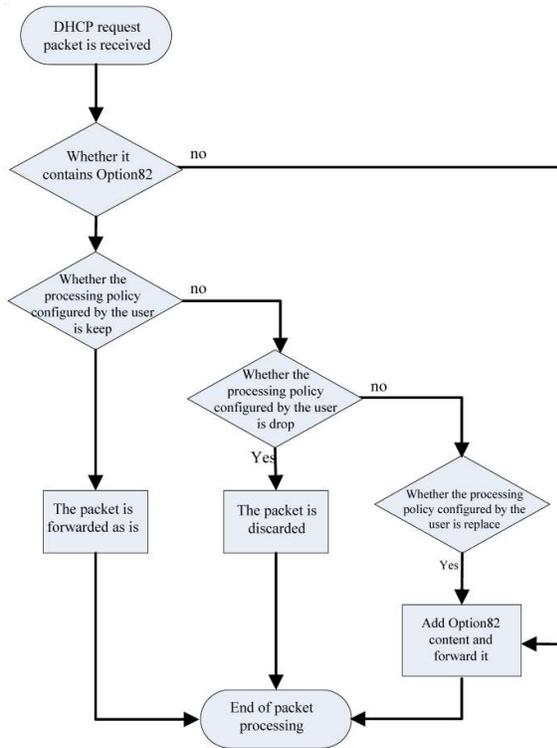


Figure 1 Processing Flow of Option82

2. When the device receives a response packet from the DHCP server, if the packet contains Option82, Option 82 is deleted and the packet is forwarded to the DHCP client. If the packet does not contain Option 82, it is directly forwarded to the DHCP client.

## 87.2 DHCP Snooping Function Configuration

Table 87 DHCP Snooping Function Configuration List

Configuration Task	
Configure Basic Functions of DHCP snooping	Configure DHCP Snooping Function
	Configure Trust Status of Port
	Configure Rate Limiting Function for DHCP Snooping

Configuration Task	
Configure DHCP snooping Option82	Configure Processing Policy of Option82
	Configure Content of Remote ID
	Configure Content of Circuit ID
	Configure Fill Format of Option82
	Configure Packet Processing Policy of Option82
Configure Binding Entries Storage for ND Snooping	Configure Automatic Storage of Binding Entries for DHCP Snooping
	Configure Manual Storage of Binding Entries for DHCP Snooping

### 87.2.1 Configure Basic Functions of DHCP snooping

The basic functions of DHCP snooping include enabling DHCP snooping, configuring trust status of port, and limiting DHCP packet rate.

#### Configuration Condition

None

#### Configure DHCP Snooping Function

After the DHCP snooping function is enabled, the DHCP packets received by all ports of the device will be monitored:

- For the request packets received, corresponding binding entries will be generated according to the information in the packets;
- For the response packets received from the trusted port, the status and lease time of corresponding binding entries will be updated;
- The response packets received from the untrusted port will be directly discarded.

Table 1 Configure DHCP Snooping Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable the DHCP snooping function	<b>dhcp-snooping</b>	Mandatory By default, the DHCP snooping function is disabled.

### Configure Trust Status of Port

To prevent the DHCP client from obtaining addresses from illegal DHCP server, you can configure the port directly or indirectly connected to legitimate server as a trusted one.

When the port is configured as a trusted one, the DHCP response packets are permitted to be normally forwarded; otherwise, they will be discarded.

Table 2 Configure Trust Status of Port

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Configure Trust Status of Port	<b>dhcp-snooping trust</b>	Mandatory By default, all ports are untrusted ones.

---

 **Note**

- The port connected to DHCP server must be configured as a trusted one; otherwise, the DHCP client cannot obtain any address.
  - After the port is configured as a trusted one, it will not limit the rate of the DHCP packets that pass through this port.
  - After the port status is changed to untrusted from trusted, the upper limit of the port rate is 40 by default.
- 

### Configure Rate Limiting Function for DHCP Snooping

Configuring rate limiting function for DHCP Snooping can limit the number of DHCP packets processed per second. This can avoid the following circumstance: other protocol packets cannot be processed in a timely manner due to the processing of DHCP packets in long term.

When the number of DHCP packets received in one second exceeds the upper limit of rate, subsequent DHCP packets will be discarded. If the DHCP packets continuously received by the port in 20 seconds all exceed the rate limit, corresponding port will be closed to isolate the source of packet impact.

Table 3 Configuring Rate Limiting Function of DHCP Snooping

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected. After you enter the layer-2 Ethernet interface
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.

Step	Command	Description
Configure Rate Limiting Function for DHCP Snooping	<b>dhcp-snooping rate-limit</b> <i>limit-value</i>	Mandatory  By default, the upper limit of the rate of DHCP packet is 40pps.

---

### Note

- After configuring the upper limit of the rate of DHCP packet in aggregation group configuration mode, it is applicable to each member port of the aggregation group.
  - The DHCP packet rate limiting function is effective for untrusted port only.
  - After the port is automatically closed, it can be automatically enabled by configuring Error-Disable. By default, the port auto closing function is enabled; if the DHCP packets received by the port exceed the rate limit for 20 consecutive seconds, and corresponding port cannot be automatically closed, you need to check the Error-Disable configuration. For the Error-Disable function, refer to the Error-Disable-related chapters in the User Manual.
- 

## 87.2.2 Configure DHCP snooping Option82

The DHCP snooping function supports Option82 which can contain 255 sub-options at most. Our company's devices support two sub-options, i.e. Circuit ID and Remote ID.

### Configuration Condition

Before configuring the DHCP snooping Option82, do the following:

- Enable the DHCP snooping function.

### Configure Processing Policy of Option82

When disabling information is configured on the port, all the option packets received by the port will be forwarded as is.

Table 4 Configuring Processing Policy of Option82

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Enable Option82 of DHCP Snooping	<b>dhcp-snooping information enable</b>	Mandatory  By default, Option82 of DHCP Snooping function is disabled.
Enter the layer-2 Ethernet interface configuration mode.	<b>interface <i>interface-name</i></b>	At least one option must be selected.  After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation <i>link-aggregation-id</i></b>	
Configure Processing Policy of Option82	<b>dhcp-snooping information disable</b>	Optional  By default, the processing policy for the DHCP request packets containing Option82 is replace, i.e. replace prior to forwarding.

### Configure Content of Remote ID

The content of Remote ID has two types, i.e. default and non-default. The default fill format of Remote ID is shown as follows:

#### Remote ID Suboption Frame Format

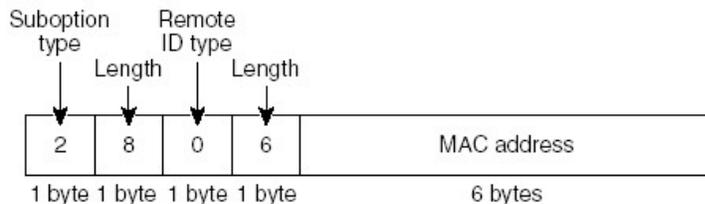


Figure 2 Fill Format of Default Remote ID Content

Non-default content has two types, i.e. custom character string and device name. It is required to be configured in the fill format to take effect under user configuration format. The fill format of the non-default Remote ID content is shown as follows:

**Remote ID Suboption Frame Format (for user-configured string):**

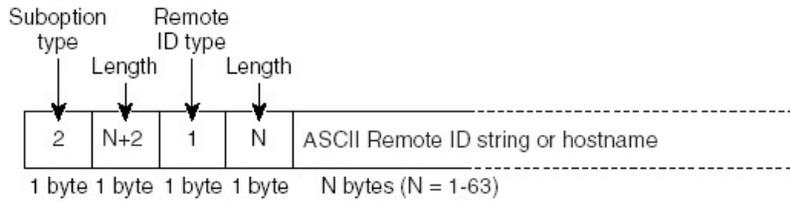


Figure 3 Fill Format of Non-default Remote ID Content

Table 5 Configure Content of Remote ID

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure Content of Remote ID	<b>dhcp-snooping information format remote-id { string   default   hostname }</b>	Mandatory By default, the content of Remote ID is default content, i.e. the MAC address of device port.

**Configure Content of Circuit ID**

The content of Circuit ID has two types, i.e. default and non-default. The fill format of the default Circuit ID content is shown as follows:

**Circuit ID Suboption Frame Format**

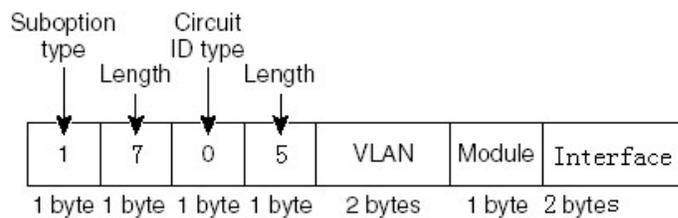


Figure 4 Fill Format of Default Circuit ID Content

Non-default content needs to be configured in the fill format to take effect under user configuration format. The fill format of the non-default Circuit ID content is shown as follows:

### Circuit ID Suboption Frame Format (for user-configured string):

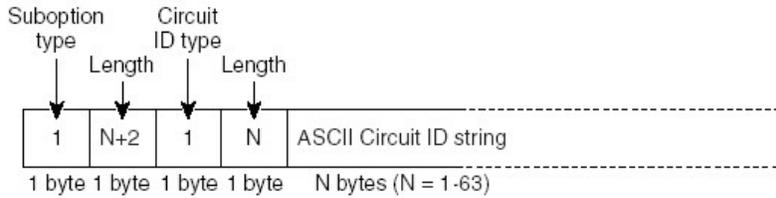


Figure 5 Fill Format of Non-default Circuit ID Content

Table 6 Configure Content of Circuit ID

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Configure Content of Circuit ID	<b>dhcp-snooping information</b> <b>format circuit-id</b> { <i>string</i>   <b>default</b> }	Mandatory  By default, the content of Circuit ID is default content.

### Configure Fill Format of Option82

The fill format of Option82 has two types, default format and user configuration format.

When the fill format is default format, the content of both Remote ID and Circuit ID is default content; only when the fill format is configured as user configuration format will the non-default content of Remote ID and Circuit ID take effect.

Table 7 Configuring Fill Format of Option82

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure Fill Format of Option82	<b>dhcp-snooping information format { default   user-config }</b>	Mandatory By default, the fill format is default format.

### Configure Packet Processing Policy of Option82

Configure the packet processing policy of Option82. You may take different forwarding policies for the DHCP request packets containing Option82.

Table 8 Configuring Packet Processing Policy of Option82

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure Packet Processing Policy of Option82	<b>dhcp-snooping information policy { drop   keep   replace }</b>	Mandatory By default, the processing policy is replace.

### 87.2.3 Configure Binding Entries Storage for ND Snooping

The DHCP snooping function supports automatic or manual storage of binding entries in the specified path. If the device restarts, the stored binding entries can be restored to prevent the communication from being affected due to the loss of binding entries.

The specified path can be device FLASH, FTP server or TFTP server.

#### Configuration Condition

Before configuring the binding entries storage path as FTP/TFTP server, do the following:

- Normally, the FTP/TFTP server function is enabled on the FTP/TFTP server;
- The device can ping the IP address of FTP/TFTP server.

#### Configure Automatic Storage of Binding Entries for DHCP Snooping

The binding entries of DHCP snooping can be configured as auto storage mode, i.e. the system stores the binding entries by timing.

The system periodically refreshes the binding entries to detect whether the binding entries have been updated. If yes, the updated entries will be stored in the specified path only after the storage delay expires. Storage delay can prevent and control frequent system storage due to the continuous updating of entries.

Table 9 Configure Auto Storage of Binding Entries of DHCP Snooping

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure Automatic Storage of Binding Entries for DHCP Snooping	<b>dhcp-snooping database savetype auto</b> { <b>flash</b> <i>file-name</i>   <b>ftp</b> <i>dest-ip-address ftp-username ftp-password file-name</i>   <b>tftp</b> <i>dest-ip-address file-name</i> }	Mandatory  By default, the binding entries storage mode is auto mode, storage path flash, and storage file name "dhcsp_binding.db".
Configure binding entries storage delay	<b>dhcp-snooping database savedelay</b> <i>seconds</i>	Optional  By default, the binding entries storage delay is 1800 seconds.
Configure binding entries refresh interval	<b>dhcp-snooping database savepool</b> <i>seconds</i>	Optional  By default, the binding entries refresh interval is 30 seconds.

### Configure Manual Storage of Binding Entries for DHCP Snooping

The binding entries of DHCP snooping can be configured as manual storage mode, i.e. the binding entries are stored by executing a storage command.

Table 10 Configure Manual Storage of Binding Entries of DHCP Snooping

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Configure Manual Storage of Binding Entries for DHCP Snooping	<b>dhcp-snooping database savetype manual</b> { <b>flash</b> <i>file-name</i>   <b>ftp</b> <i>dest-ip-address ftp-username ftp-password file-name</i>   <b>tftp</b> <i>dest-ip-address file-name</i> }	Mandatory  By default, the binding entries storage mode is auto mode, storage path flash, and storage file name "dhcsp_binding.db".
Configure storage binding files	<b>dhcp-snooping database save</b>	Mandatory  Store binding entries in the specified path  By default, the binding entries are not stored in the specified path.

## 87.2.4 DHCP Snooping Monitoring and Maintaining

Table 11 DHCP Snooping Monitoring and Maintaining

Command	Description
<b>clear dhcp-snooping database</b> { <b>interface</b> { <i>interface-list</i>   <b>link-aggregation</b> <i>link-aggregation-id</i> }   <b>ip-address</b> <i>ip-address</i>   <b>mac-address</b> <i>mac-address</i>   <b>vlan</b> <i>vlan-id</i>   <b>all</b> }	Clear binding entries
<b>clear dhcp-snooping packet statistics</b> [ <b>interface</b> { <i>interface-name</i>   <b>link-aggregation</b> <i>link-aggregation-id</i> } ]	Clear statistics of receiving and sending DHCP packets
<b>show dhcp-snooping</b> [ <b>interface</b> { <i>interface-name</i>   <b>link-aggregation</b> <i>link-aggregation-id</i> }   <b>save</b>   <b>detail</b> ]	#Show the configuration information of DHCP Snooping
<b>show dhcp-snooping database</b> [   { { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>expression</i>   <b>redirect</b> { <b>file</b> <i>file-name</i>   <b>ftp</b> [ <b>vrf</b> <i>vrf-name</i> ] { <i>hostname</i>   <i>dest-ip-address</i> } <i>ftp-username ftp-password file-name</i> } } ] [ <b>interface</b> { <i>interface-name</i>   <b>link-</b>	Show the information about binding entries of DHCP Snooping

Command	Description
<b>aggregation</b> <i>link-aggregation-id</i> }   <b>ip-address</b> <i>ip-address</i>   <b>vlan</b> <i>vlan-id</i>   <b>mac-address</b> <i>mac-address</i> [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>expression</i>   <b>redirect</b> { <b>file</b> <i>file-name</i>   <b>ftp</b> [ <b>vrf</b> <i>vrf-name</i> ] { <i>hostname</i>   <i>dest-ip-address</i> } <i>ftp-username</i> <i>ftp-password</i> <i>file-name</i> } } ]   <b>detail</b> ]	
<b>show dhcp-snooping packet statistics</b> [ <b>interface</b> { <i>interface-name</i>   <b>link-aggregation</b> <i>link-aggregation-id</i> } ]	Show the statistics of receiving and sending DHCP packets

## 87.3 Typical Configuration Example of DHCP Snooping

### 87.3.1 Configure Basic Functions of DHCP Snooping

#### Network Requirements

- DHCP Server1 is a legal DHCP server, and DHCP Server2 is an illegal DHCP server.
- After the DHCP snooping function is configured, both PC1 and PC2 can obtain addresses from DHCP Server1 only.

#### Network Topology

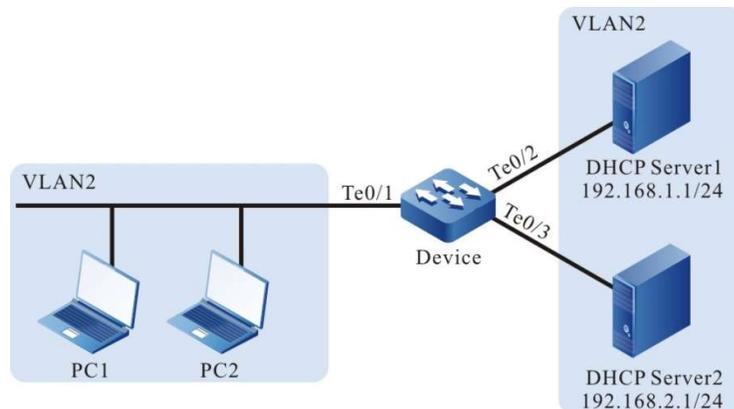


Figure 6 Network Topology for Configuring Basic Functions of DHCP Snooping

#### Configuration Steps

Step 1: Configure VLAN and port link type on Device.

#Create VLAN 2.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the link type of ports tengigabitethernet0/1~tengigabitethernet0/3 as Access, allowing the services of VLAN2 to pass.

```
Device(config)#interface tengigabitethernet 0/1-0/3
Device(config-if-range)#switchport mode access
Device(config-if-range)#switchport access vlan 2
Device(config-if-range)#exit
```

Step 2: Configure the address pool of DHCP Server1 as 192.168.1.100~192.168.1.199 and that of DHCP Server2 as 192.168.2.100~192.168.2.199. (omitted)

Step 3: Configure DHCP Snooping function on the Device.

#Enable the DHCP snooping function.

```
Device(config)#dhcp-snooping
```

#Configure the port tengigabitethernet0/2 as a trusted port.

```
Device(config)#interface tengigabitethernet 0/2
Device(config-if-tengigabitethernet0/2)#dhcp-snooping trust
Device(config-if-tengigabitethernet0/2)#exit
```

Step 4: Check the result.

#After both PC1 and PC2 successfully obtain the address, view the entries of DHCP Snooping on the Device.

```
Device#show dhcp-snooping database
dhcp-snooping database:
database entries count:2
database entries delete time :300
-----
 macAddr    ipAddr    transtion-id  vlan  interface  leaseTime(s)  status
-----
0013.0100.0002  192.168.1.101  1      2    te0/1      107990    active
-----
0013.0100.0001  192.168.1.100  0      2    te0/1      107989    active
-----
Total valid DHCP Client binding table for this criterion: 2
```

Both PC1 and PC2 can obtain addresses from DHCP Server1 only.

# 88 DHCPv6 Snooping

---

## 88.1 Overview

### 88.1.1 Basic Functions of DHCPv6 Snooping

DHCPv6 snooping is a security feature of DHCPv6 (Dynamic Host Configuration Protocol for IPv6). It has the following two functions:

1. Record the corresponding relation between MAC address and IPv6 address of DHCPv6 client:

For the sake of security, the network administrator may need to record the IPv6 address used when users surf the Internet, and confirm the corresponding relation between the MAC address of users' host and the IPv6 address obtained from the DHCPv6 server.

DHCPv6 snooping records the MAC address of DHCPv6 client and the IPv6 address obtained by snooping DHCPv6 request packets and the DHCPv6 response packets received by the trusted port. The administrator may view the IPv6 address information obtained by the DHCPv6 client through the binding entries recorded by DHCPv6 snooping.

2. Guarantee the client obtains IPv6 address from a legitimate server:

If there is DHCPv6 server set up in the network without permission, the DHCPv6 client is likely to obtain incorrect IPv6 address, causing abnormal communication or safety hazard. In order to ensure that the DHCPv6 client can obtain IPv6 address through a legitimate DHCPv6 server, the DHCPv6 snooping function permits the port to be configured as a trusted or an untrusted one:

- Trusted port is directly or indirectly connected to a legitimate DHCPv6 server. Trusted port normally forwards the DHCPv6 response packets received so as to ensure that the DHCPv6 client can obtain a correct IPv6 address;
- An untrusted port is not directly or indirectly connected to a legitimate DHCPv6 server. If a DHCPv6 response packet sent by the DHCPv6 server is received from an untrusted port, it will be discarded to prevent the DHCPv6 client from obtaining incorrect IPv6 address.

### 88.1.2 DHCPv6 Snooping Option18/37

In order that the DHCPv6 Server can obtain the physical location of DHCPv6 client, Option18 and Option37 can be added to the DHCPv6 request packet.

When the device is snooping DHCPv6 packets, some user-related device information can be added to the DHCPv6 request packet in DHCPv6 Option mode. In particular, Option18 which records the interface information of the client is called Interface ID option. Option37 recording the MAC address information of the client is called Remote ID option.

When Option18/37 is enabled, after the device receives the DHCPv6 request packets, it may process them by the following manners according to the processing policy and fill method of Option18/37 configured by users:

Table 88-1 DHCPv6 Request Packet Processing Policy

DHCPv6 request packet	Processing policy	Fill method	Packet processing principle
Without Option18/37	Add	Default fill format	Fill and forward in default format
	Add	Extend fill format	Fill and forward in the user-defined format
With Option18/37	maintained	Not filled	No processing or forwarding of Option18/37
	Replacements	Default fill format	Replace the original Option18/37 in default format and forward
		Extend fill format	Replace the original Option18/37 in the user-defined format and forward

## 88.2 DHCPv6 Snooping Function Configuration

Table 1 DHCPv6 Snooping Function Configuration List

Configuration Task	
Configure Basic Functions of DHCPv6 Snooping	Enable DHCPv6 Snooping
	Configure Trust Status of Port
	Configure Number of Binding Entries of Port
Configure DHCPv6 Snooping Option18/37	Configure Option18

Configuration Task	
	Configure Option37
	Configure Packet Processing Policy of Option18/37
Configure Delay Time of Deleting Invalid Entries of DHCPv6 Snooping	Configure Delay Time of Deleting Invalid Entries of DHCPv6 Snooping
Configure Storage of Binding Entries of DHCPv6 Snooping	Configure Storage of Binding Entries of DHCPv6 Snooping

### 88.2.1 Configure Basic Functions of DHCPv6 Snooping

The basic functions of DHCPv6 snooping include enabling DHCPv6 snooping, configuring trust status of port, and configuring the number of DHCPv6 snooping entries bound to the port.

#### Configuration Condition

None

#### Enable DHCPv6 Snooping

After the DHCPv6 snooping function is enabled, the DHCPv6 packets received by all ports of the device will be monitored:

- For the DHCPv6 request packets received, corresponding binding entries will be generated according to the information in the packets;
- For the response packets received from the trusted port, the status and lease time of corresponding binding entries will be updated;
- The response packets received from the untrusted port will be directly discarded.

Table 2 Enabling DHCPv6 Snooping

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable DHCPv6 snooping	<b>ipv6 dhcp snooping enable</b>	At least one option must be selected.

Step	Command	Description
Enable the DHCPv6 snooping function of the specified VLAN	<b>ipv6 dhcp snooping</b> <b>vlan <i>vlanlist</i></b>	By default, the DHCPv6 snooping function is disabled.

### Configure Trust Status of Port

To prevent the DHCPv6 client from obtaining addresses from illegal DHCPv6 server, you can configure the port directly or indirectly connected to legitimate server as a trusted one.

When the port is configured as a trusted one, the DHCPv6 response packets are permitted to be normally forwarded; otherwise, they will be discarded.

Table 3 Configuring Trust Status of Port

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface <i>interface-name</i></b>	At least one option must be selected.  After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <b><i>link-aggregation-id</i></b>	
Configure Trust Status of Port	<b>ipv6 dhcp snooping trust</b>	Mandatory  By default, all ports are untrusted ones.



**Note**

- The port connected to DHCPv6 server must be configured as a trusted one; otherwise, the DHCPv6 client cannot obtain any address.

### Configure the Number of Binding Entries of Port DHCPv6 Snooping

Configure the number of binding entries of DHCPv6 snooping. You can limit the maximum number of dynamic entries to be learned by the port to prevent them from occupying too many resources.

Table 4 Configuring Number of Binding Entries of Port DHCPv6 Snooping

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Configure the number of binding entries of DHCPv6 snooping	<b>ipv6 dhcp snooping max-learning-num</b> <i>number</i>	Mandatory  By default, 1024 binding entries can be learned by the port.

### 88.2.2 Configure DHCPv6 Snooping Option18/37

The DHCPv6 snooping function supports Option18 and Option37, both of which support the default and extended fill format.

#### Configuration Condition

Before configuring the DHCP snooping Option18 and Option37, do the following:

- Enable the DHCPv6 snooping function.

### Configure Option18

The content of Interface ID has two types of fill format, i.e. default and extended. The fill format of the default Interface ID content is shown as follows:

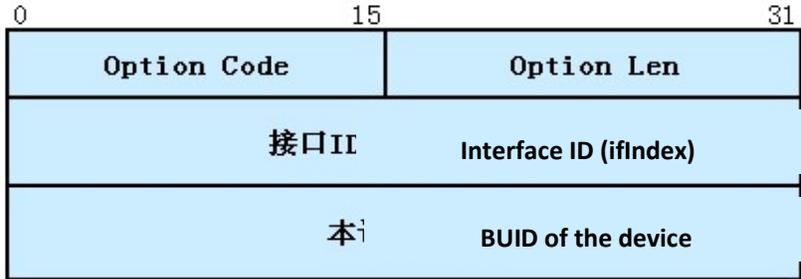


Figure 88 Fill Format of Default Interface ID Content

For the extended fill format, the fill format needs to be configured to take effect under user configuration format. The extended fill format of the Interface ID content is shown as follows:



Figure 88 Extended Fill Format of Interface ID

Table 5 Configuring Option18

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect

Step	Command	Description
		only within the aggregation group.
Enable the Option18 function	<b>ipv6 dhcp snooping option interface-id enable</b>	Mandatory By default, the Option18 function is disabled.
Configure the content of Interface ID option	<b>ipv6 dhcp snooping option format interface-id <i>string</i></b>	Optional By default, the content of Interface ID in Option18 is in interface id - duid format.

### Configure Option37

The content of Remote ID has two types of fill format, i.e. default and extended. The default fill format of Remote ID is shown as follows:

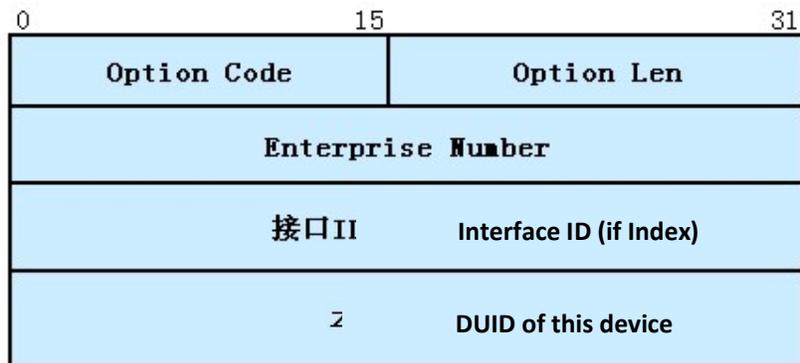


Figure 88 Fill Format of Default Remote ID Content

For the extended fill format, the fill format needs to be configured to take effect under user configuration format. The extended fill format of the Remote ID content is shown as follows:

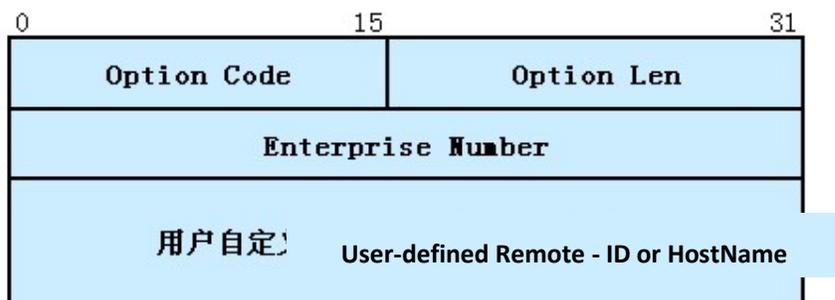


Figure 1 Fill Format of Non-default Remote ID Content

Table 6 Configuring Option37

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enable the Option37 function	<b>ipv6 dhcp snooping option remote-id enable</b>	Mandatory By default, the Option37 function is disabled.
Configure Content of Remote ID	<b>ipv6 dhcp snooping option format remote-id</b> { <i>string</i>   <b>hostname</b> }	Mandatory By default, the content of Remote ID in Option37 is in enterprise num - interface id-duid format.

**Configure Packet Processing Policy of Option18/37**

Configure the packet processing policy of Option18/37. You may take different processing policies for the DHCPv6 request packets containing Option18/37.

Table 7 Configuring Packet Processing Policy of Option18/37

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Configure Packet Processing Policy of Option18/37	<b>ipv6 dhcp snooping option policy replace</b>	Mandatory  By default, the content of Option18/37 in DHCPv6 request packets is not replaced.

### 88.2.3 Configure Delay Time of Deleting Invalid Entries of DHCPv6 Snooping

#### Configuration Condition

Before configuring the delay time of deleting invalid binding entries for DHCPv6 snooping, do the following:

- Enable the DHCPv6 snooping function.

#### Configure Delay Time of Deleting Invalid Entries of DHCPv6 Snooping

After the binding relation is cancelled, the binding entries are updated as invalid. These invalid entries will not be deleted until the delay time expires. During this period of time, if the client renews the lease, they can be reactivated without reestablishing binding entries.

Table 8 Configuring Delay Time of Deleting Invalid Entries of DHCP Snooping

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure Delay Time of Deleting Invalid Entries of DHCPv6 Snooping	<b>ipv6 dhcp snooping database timeout</b> <i>seconds</i>	Mandatory By default, the delay time of deleting invalid binding entries is 300 seconds.

## 88.2.4 Configure Storage of Binding Entries of DHCPv6 Snooping

The DHCPv6 snooping function supports automatic storage of binding entries in FLASH. If the device restarts, the stored binding entries can be restored to prevent the communication from being affected due to the loss of binding entries.

### Configuration Condition

Before configuring the storage of binding entries of DHCPv6 snooping, do the following:

- Enable the DHCPv6 snooping function.

### Configure Storage of Binding Entries of DHCPv6 Snooping

The system periodically refreshes the binding entries of DHCPv6 snooping to detect whether the binding entries have been updated. If yes, the updated entries will be automatically stored in the specified path after the storage delay expires. At the same time, the binding entries may also be stored in FLASH immediately.

Table 9 Configuring Storage of Binding Entries of DHCPv6 Snooping

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the refresh interval of binding entries of DHCPv6 snooping	<b>ipv6 dhcp snooping database save pool</b> <i>seconds</i>	Optional By default, the refresh interval of binding entries is 30 seconds.
Configure the storage delay of binding entries of DHCPv6 snooping	<b>ipv6 dhcp snooping database save interval</b> <i>seconds</i>	Optional By default, the binding entries storage delay is 1800 seconds.

Step	Command	Description
Configure to perform storage of binding entries immediately	<b>ipv6 dhcp snooping database save now</b>	Optional By default, the storage delay of binding entries is 1800 seconds.
Configure the storage of binding entries of DHCPv6 snooping in the specified file	<b>ipv6 dhcp snooping database save filename</b> <i>string</i>	Mandatory By default, the name of the storage file is "/flash/dhcpv6sp_binding.db".

## 88.2.5 DHCPv6 snooping monitoring and maintaining

Table 10 DHCPv6 Snooping Monitoring and Maintaining

Command	Description
<b>clear ipv6 dhcp snooping database</b> [ <b>interface</b> { <i>interface-list</i> }   <b>ipv6-address</b> <i>ipv6-address</i>   <i>mac-address</i>   <b>vlan</b> <i>vlan-id</i> ]	Clear binding entries of DHCPv6 Snooping
<b>clear ipv6 dhcp snooping statistics</b> [ <b>interface</b> { <i>interface-name</i> } ]	Clear the statistics of receiving and sending DHCPv6 packets
<b>show ipv6 dhcp snooping</b> [ <b>interface</b> { <i>interface-name</i> } ]	#Show DHCPv6 Snooping-related configuration information on the specified interface
<b>show ipv6 dhcp snooping database</b> [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>expression</i>   <b>redirect</b> { <b>file</b> <i>file-name</i>   <b>ftp</b> [ <b>vrf</b> <i>vrf-name</i> ] { <i>hostname</i>   <i>dest-ip-address</i> } <i>ftp-username</i> <i>ftp-password</i> <i>file-name</i> } } ] [ <b>interface</b> { <i>interface-name</i> }   <b>ipv6-address</b> <i>ipv6-address</i>   <b>mac-address</b> <i>mac-address</i>   <b>vlan</b> <i>vlan-id</i> ] [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>expression</i>   <b>redirect</b> { <b>file</b> <i>file-name</i>   <b>ftp</b> [ <b>vrf</b> <i>vrf-name</i> ] { <i>hostname</i>   <i>dest-ip-address</i> } <i>ftp-username</i> <i>ftp-password</i> <i>file-name</i> } } ] ]	Show the information of binding entries of DHCPv6 Snooping
<b>show ipv6 dhcp snooping statistics</b> [ <b>interface</b> { <i>interface-name</i> } ]	Show the statistics of receiving and sending DHCPv6 packets

## 88.3 Typical configuration example of DHCPv6 Snooping

### 88.3.1 Configure Basic Functions of DHCPv6 Snooping

#### Network Requirements

- DHCPv6 Server1 is a legitimate DHCPv6 server, and DHCPv6 Server2 is an illegal DHCPv6 server.
- After the DHCPv6 snooping function is configured, both PC1 and PC2 can obtain addresses from DHCPv6 Server1 only.

#### Network Topology

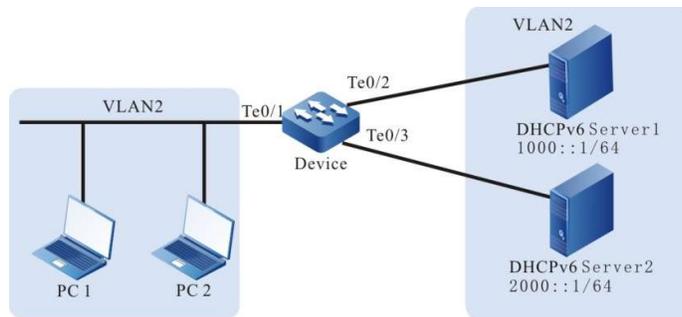


Figure 2 Network Topology for Configuring Basic Functions of DHCPv6 Snooping

#### Configuration Steps

Step 1: Configure VLAN and port link type on Device.

```
#Create VLAN 2.
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the link type of ports tengigabitethernet0/1~tengigabitethernet0/3 as Access, allowing the services of VLAN2 to pass.

```
Device(config)#interface tengigabitethernet 0/1-0/3
Device(config-if-range)#switchport mode access
Device(config-if-range)#switchport access vlan 2
Device(config-if-range)#exit
```

Step 2: Configure the address pool of DHCPv6 Server1 as 1000::2/64 and that of DHCP Server2 as 2000::2/64. (omitted)

Step 3: Configure the DHCPv6 Snooping function on the Device.

#Enable the DHCPv6 snooping function.

```
Device(config)#ipv6 dhcp snooping enable
```

#Configure the port tengigabitethernet0/2 as a trusted port.

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-tengigabitethernet0/2)#ipv6 dhcp snooping trust
Device(config-if-tengigabitethernet0/2)#exit
```

Step 4: Check the result.

#After both PC1 and PC2 successfully obtain the address, view the entries of DHCPv6 Snooping on the Device.

```
Device#show ipv6 dhcp snooping database
Interface-Name  MAC-Address  VLAN-ID  ValidTime  AgedTime  IP-Address
te0/1           0001.0001.0008  2        120        0         1000::2
te0/1           0001.0001.0007  2        120        0         1000::3
```

Both PC1 and PC2 can obtain addresses from DHCPv6 Server1 only.

# 89 Dynamic ARP Inspection

---

## 89.1 Overview

Dynamic ARP Inspection is called DAI function for short. It can increase network security by detecting the legality of ARP (Address Resolution Protocol) packets to discover and prevent ARP spoofing attack. The DAI function has two types:

- Port DAI: Detect the legality of the ARP packets received by the specified port to discover and prevent ARP spoofing attack;

The legality of ARP packets is checked according to the binding entries of port IP Source Guard. The specific principle is shown below:

For the ARP packets received, if the IP address of sending end, source MAC address and VLAN ID fully match the entries bound to the ARP Check of the port, these ARP packets are legal and forwarded; otherwise, they are illegal and discarded, and the log information is recorded.

- Global DAI: Detect the legality of all ARP packets received by the port to prevent fake users from sending fake ARP packets so that the device establishes incorrect ARP entries.

The legality of ARP packets is checked according to the binding entries of global IP Source Guard. The specific principle is shown below:

For the ARP packets received, if the IP address of sending end is the same as that in the binding entries of global IP Source Guard yet the MAC address is different, these ARP packets are considered fake and discarded, and the log information is not recorded.

The port DAI and global DAI function can also check the legality of ARP packets. The specific principle is shown below:

If the source MAC address in the ARP packets received is different from the MAC address of the sending end, these packets are invalid ones and discarded, and the log information is not recorded.

- Detection of port ARP attack: record the log information instead of detecting the legality of the ARP packets received by the specified to look for ARP attack.

## 89.2 Dynamic ARP Inspection function configuration

Table 89-1 Dynamic ARP Inspection Function Configuration List

Configuration Task	
Configure Dynamic ARP Inspection Function of Port	Configure Dynamic ARP Inspection Function of Port
Configure Global Dynamic ARP Inspection Function	Configure Global Dynamic ARP Inspection Function

### 89.2.1 Configure Dynamic ARP Inspection Function of Port

#### Configuration Condition

Before configuring Dynamic ARP Inspection function of port, the following tasks should be completed:

- Configure binding entries for port IP Source Guard.

#### Configure Dynamic ARP Inspection Function of Port

After the port DAI function is enabled, the system will check the legality of the ARP packets received by this port according to the binding entries of port IP Source Guard. Illegal packets will be discarded and recorded in the log.

The content recorded in the log includes VLAN ID, receiving port, IP address of sending end, destination IP address, MAC address of sending end, destination MAC address, and the number of identical ARP packets. Users may make further analysis according to the log information recorded, such as locating the host initiating ARP attack.

By default, log information is output on a periodic basis. The recording, output and aging of packets can be controlled by configuring log output interval. Log output interval serves as the basic value of the following log-related parameter:

- Log refresh cycle: Identify whether the log needs to be output or has been aged. If the log output interval configured is less than 5 seconds, the log refresh cycle is 1 second; otherwise, the log refresh cycle is one fifth of the log output interval;
- Log aging time: After the aging time expires, the log will be deleted. The log aging time is twice the log output interval;
- Log token: During the log refresh cycle, the allowable maximum number of logs. The number of log tokens is 15 times the value of log refresh cycle.

After the port DAI function is enabled, you can also configure rate limiting function for port ARP, i.e., limiting the number of ARP packets processed per second to prevent the system from processing a large number of ARP packets for a long time so that other protocol packets cannot be processed in a timely manner.

---

 **Note**

- The rate limiting function of port ARP, i.e. limiting the number of ARP packets processed per second to prevent the system from processing a large number of ARP packets for a long time so that other protocol packets cannot be processed in a timely manner. When the number of ARP packets received in one second exceeds the upper limit of rate, subsequent ARP packets received will be discarded. If the ARP packets continuously received by the port in 20 seconds all exceed the rate limit, corresponding port will be closed to isolate the source of packet impact.
- 

Table 89 Configuring Dynamic ARP Inspection of the Port

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Enable the DAI function of the port	<b>ip arp inspection</b>	Mandatory  By default, the DAI function of the port is disabled.

Step	Command	Description
Configure the upper limit of processing ARP packets by the port	<b>ip arp inspection rate-limit</b> <i>limit-value</i>	Optional By default, the upper limit of processing ARP packets by the port is 15pps.
Return to the global configuration mode	<b>exit</b>	-
Configure the number of cache logs	<b>ip arp inspection log-buffer</b> <i>buffer-size</i>	Optional By default, the system can cache 32 logs. If it is configured as 0, no log is cached, i.e. the log is directly output to the terminal after an illegal ARP packet is detected.
Configure the log output interval	<b>ip arp inspection log-interval</b> <i>seconds</i>	Optional By default, the log output interval is 20 seconds. If it is configured as 0, the log is output immediately, i.e. the log is directly output to the terminal after an illegal ARP packet is detected.
Configure the log output level	<b>ip arp inspection log-level</b> <i>log-level</i>	Optional By default, the log output level is 6.

## Note

- After the DAI function is enabled, all the ARP packets (broadcast and unicast ARP) received by corresponding port are redirected to CPU for detection, software forwarding and log recording. When there are a large number of ARP packets, they will consume a lot of CPU resources. Therefore, when the device communication is normal, enabling the DAI function of the port is not recommended. Only when you suspect ARP spoofing attack occurs in the network will the DAI function of the port be enabled for detection and locating.
- Under the same port, the port DAI function cannot be enabled simultaneously with the port

---

security function.

- After configuring the upper limit of the rate of APR packet processed by the port in aggregation group configuration mode, it is applicable to each member port of the aggregation group.
  - If the ARP packets received by the port in 20 consecutive seconds exceed the upper limit, and the port is not closed automatically, you should refer to Error-Disable-related chapters in the User Manual.
- 

## 89.2.2 Configure Global Dynamic ARP Inspection Function

### Configuration Condition

Before configuring global Dynamic ARP Inspection function, the following tasks should be completed:

- Configure the binding entries of global IP Source Guard.

### Configure Global Dynamic ARP Inspection Function

After the global DAI function is enabled, the system will check the legality of the ARP packets received by this port according to the binding entries of global IP Source Guard. Illegal packets will be discarded directly without being recorded in the log.

Table 1 Configuring Global Dynamic ARP Inspection Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable global DAI function	<b>arp-security</b>	Mandatory By default, the global DAI function is disabled.

## 89.2.3 Configure Dynamic ARP Inspection to Detect ARP Attack

### Configuration Condition

None

### Configure Dynamic ARP Inspection to detect ARP attack

After ARP attack detection is enabled, the system will record log instead of checking the legality of ARP packets received.

Table 89-4 Configuring Dynamic ARP Inspection to Detect ARP Attack

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Enable ARP attack detection of the port	<b>ip arp inspection attack</b>	Mandatory  By default, ARP attack detection is disabled on the port.

## 89.2.4 Dynamic ARP Inspection Monitoring and Maintaining

Table 89-5 Dynamic ARP Inspection Monitoring and Maintaining

Command	Description
<b>clear ip arp inspection</b> { <b>log-information</b>   <b>log-statistics</b>   <b>pkt-statistics</b> [ <b>interface</b> { <i>interface-name</i>   <b>link-aggregation</b> <i>link-aggregation-id</i> } ] }	Delete the statistics of DIA function record
<b>show arp-security</b>	Show the status of global DAI function
<b>show ip arp inspection</b> [ <b>interface</b> { <i>interface-name</i>   <b>link-aggregation</b> <i>link-aggregation-id</i> } ]	Show the configuration information of port DAI function

Command	Description
<b>show ip arp inspection log-information</b>	Show the log information of port DIA function record
<b>show ip arp inspection log-statistics</b>	Show the statistics of the number of logs
<b>show ip arp inspection pkt-statistics</b> [ <b>interface</b> { <i>interface-name</i>   <i>link-aggregation link-aggregation-id</i> } ]	Show the statistics of ARP packets

## 89.3 Typical Configuration Example of DAI

### 89.3.1 Configure Basic Functions of DAI

#### Network Requirements

- PC1 and PC2 access IP network through the Device.
- On the Device, configure the port DAI function to prevent from ARP attack and spoofing.

#### Network Topology

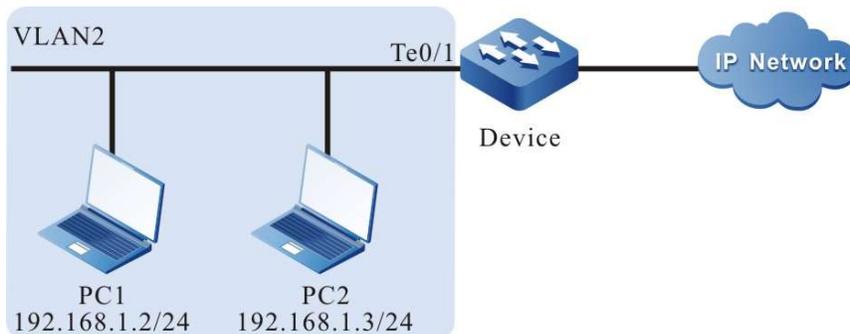


Figure 89 Network Topology for Configuring Basic Functions of DAI

#### Configuration Steps

Step 1: Configure VLAN and port link type on Device.

#Create VLAN 2.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the link type of port tengigabitethernet0/1 as Access to allow services of VLAN 2 to pass.

```

Device(config)#interface tengigabitethernet 0/1
Device(config-if-tengigabitethernet0/1)#switchport mode access
Device(config-if-tengigabitethernet0/1)#switchport access vlan 2
Device(config-if-tengigabitethernet0/1)#exit

```

Step 2: Configure port DAI function on the Device.

#Enable the port DAI function on the port tengigabitethernet0/1, and configure the upper limit of processing ARP packets by this port as 30pps.

```

Device(config)#interface tengigabitethernet 0/1
Device(config-if-tengigabitethernet0/1)#ip arp inspection
Device(config-if-tengigabitethernet0/1)#ip arp inspection rate-limit 30
Device(config-if-tengigabitethernet0/1)#exit

```

Step 3: Configure binding entries on the Device.

#On the port gigabitethernet0/1, configure the binding entries of port IP Source Guard with MAC address of 0012.0100.0001, IP address of 192.168.1.2, and VLAN of 2.

```

Device(config)#interface tengigabitethernet 0/1
Device(config-if-tengigabitethernet0/1)#ip source binding ip-address 192.168.1.2 mac-address 0012.0100.0001 vlan 2
Device(config-if-tengigabitethernet0/1)#exit

```

Step 4: Check the result.

#View DHCP-related configuration information.

```

Device#show ip arp inspection
Dynamic ARP Inspection information:
Dynamic ARP Inspection log buffer size: 30
Dynamic ARP Inspection log Interval: 20
Dynamic ARP Inspection log Level: 6
Dynamic ARP Inspection interface information :
-----
interface      status  rate-limit(pps)  attack
te0/1          enable  30                OFF
te0/2          disable 15                OFF
.....

```

#When the port tengigabitethernet0/1 receives ARP packets at a rate which is more than 30pps, the Device will discard the packets that exceed the rate and output the following prompt messages.

```

Jan 1 02:21:06: The rate on interface tengigabitethernet0/1 too fast ,the arp packet drop!

```

#When the port tengigabitethernet0/1 receives ARP packets at a rate which is more than 30pps for 20 seconds, the Device will close this port and output the following prompt messages.

```

Jan 1 02:21:26: %LINK-INTERFACE_DOWN-4: interface tengigabitethernet0/1, changed state to down
Jan 1 02:21:26: The rate of arp packet is too fast,dynamic arp inspection shut down the tengigabitethernet0/1 !

```

#Whe the ARP packets received by the port tengigabitethernet0/1 are inconsistent with the binding entries, the Device records the illegal information in the following format in the DAI log and output it periodically.

```
Jan 1 07:19:49: SEC-7-DARPLOG: sender IP address: 192.168.1.3 sender MAC address:0011.0100.0001 target IP address: 0.0.0.0 target MAC address:0000.0000.0000 vlan ID:2 interface ID: tengigabitethernet0/1 record packet :32 packet(s)
```

#View DAI log.

```
Device#show ip arp inspection log-information  
LogCountInBuffer:1
```

```
SEC-7-DARPLOG: sender IP address: 192.168.1.3 sender MAC address:0011.0100.0001 target IP address: 0.0.0.0 target MAC address:0000.0000.0000 vlan ID:2 interface ID: tengigabitethernet0/1 record packet :0 packet(s)
```

## 89.3.2 Combination of DAI with DHCP Snooping

### Network Requirements

- PC1 and PC2 access the IP Network through Device1, with PC2 being a DHCP client and Device2 being a DHCP relay.
- On Device1, configure DHCP Snooping and port DAI function so that PC2 instead of PC1 can normally access the IP Network.

### Network Topology

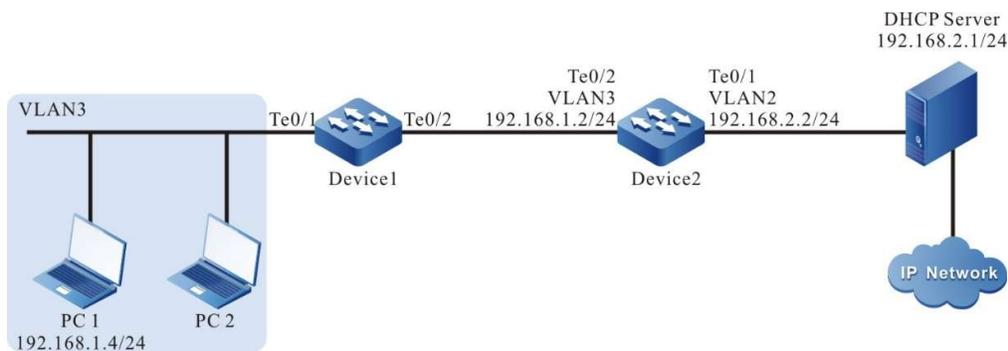


Figure 89 Network Topology for Combination of DAI and DHCP Snooping

### Configuration Steps

Step 1: Configure VLAN and port link type on Device1.

#Create VLAN3.

```
Device1#configure terminal  
Device1(config)#vlan 3  
Device1(config-vlan3)#exit
```

#Configure the link type of both tengigabitethernet0/1 and tengigabitethernet0/2 as Access, permitting the services of VLAN3 to pass.

```
Device1(config)#interface tengigabitethernet 0/1-0/2  
Device1(config-if-range)#switchport access vlan 3  
Device1(config-if-range)#exit
```

Step 2: Configure VLAN and port link type on Device2.

#Create VLAN2 and VLAN3.

```
Device2#configure terminal
Device2(config)#vlan 2-3
```

#Configure the link type of port tengigabitethernet0/1 and tengigabitethernet0/2 as Access. Port tengigabitethernet0/1 allows the services of VLAN2 to pass and tengigabitethernet0/2 allows the services of VLAN3 to pass.

```
Device2(config)#interface tengigabitethernet 0/1
Device2(config-if-tengigabitethernet0/1)#switchport mode access
Device2(config-if-tengigabitethernet0/1)#switchport access vlan 2
Device2(config-if-tengigabitethernet0/1)#exit
Device2(config)#interface tengigabitethernet 0/2
Device2(config-if-tengigabitethernet0/2)#switchport mode access
Device2(config-if-tengigabitethernet0/2)#switchport access vlan 3
Device2(config-if-tengigabitethernet0/2)#exit
```

Step 3: Configure corresponding VLAN interface and IP address on Device1 and Device2. (Omitted)

Step 4: Configure DHCP Snooping function on Device1.

#Enable the DHCP Snooping function and configure gigabitethernet0/2 as a trusted port.

```
Device1(config)#dhcp-snooping
Device1(config)#interface tengigabitethernet 0/2
Device1(config-if-tengigabitethernet0/2)#dhcp-snooping trust
Device1(config-if-tengigabitethernet0/2)#exit
```

Step 5: Configure port DAI function on Device1.

#On the port tengigabitethernet0/1, enable the port DAI function.

```
Device1(config)#interface tengigabitethernet 0/1
Device1(config-if-tengigabitethernet0/1)#ip arp inspection
Device1(config-if-tengigabitethernet0/1)#exit
```

Step 6: Configure the IP address of DHCP relay server on Device2.

#Configure the IP address of DHCP relay server as 198.168.2.1.

```
Device2(config-if-vlan3)ip dhcp relay
Device2(config-if-vlan3)ip dhcp relay server-address 192.168.2.1
```

Step 7: Check the result.

#After PC2 successfully obtains the address, view the dynamic entries of DHCP Snooping on Device1.

```
Device1#show dhcp-snooping database
dhcp-snooping database:
database entries count:1
database entries delete time :300
-----
macAddr      ipAddr      transion-id  vlan  interface  leaseTime(s)  status
0013.0100.0001 192.168.1.100  2          2    te0/1      107990        active
-----
```

#PC2 instead of PC1 can normally access the IP Network.

# 90 Host Guard

---

## 90.1 Overview

Host Guard is mainly used for the device in the access layer to prevent the ARP (Address Resolution Protocol) packets counterfeited by the attacker from damaging the ARP table on the terminal device. The host IP address protected by Host Guard generally corresponds to the IP address of the gateway device and important server in the network.

For the Host Guard function, there are two concepts:

- Host protection group: It is composed of a series of host protection group rules, i.e. the set of protected host IP address;
- Host protection group rule: A protected host IP address.

The working principle of Host Guard function is shown below:

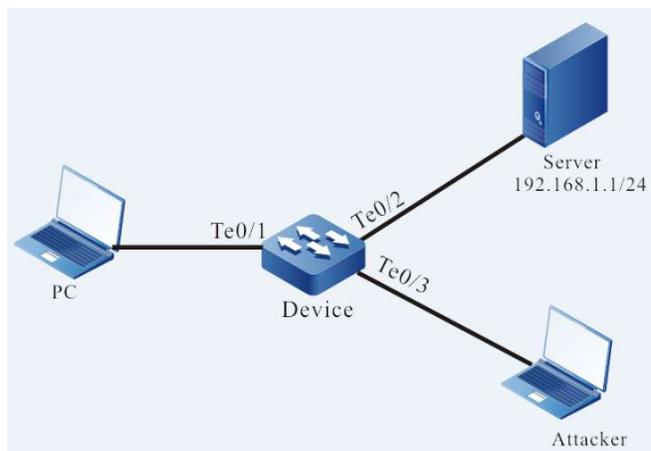


Figure 90 Functions of Host Guard

As shown in the figure above, the Attacker can use the IP address 192.168.1.1 of the Server to counterfeit ARP packets that will be forwarded to PC through the Device and damage the ARP table on the PC so that it cannot normally access the Server.

On the Device, after applying the IP address 192.168.1.1 of the Server to the port te0/2 as a host protection group rule, when among the ARP packets received by the Device, the IP address at the sending end is the same as that in the Server, if the receiving port is te0/2, the packets can be processed with normal methods; if not, they will be discarded. That is to say, the ARP packets sent by the Server can be forwarded through the port te0/2 only, and those counterfeited by the Attacker will be discarded.

## 90.2 Host Guard Function Configuration

Table 90-1 Host Guard Function Configuration List

Configuration Task	
Configure Host Guard Function	Configure Host Protection Group
	Configure Application of Host Protection Group

### 90.2.1 Configure Host Guard Function

#### Configuration Condition

None

#### Configure Host Protection Group

The host protection group is composed of a series of host protection group rules. The IP address of gateway and important server in the network can be configured as a rule in the host protection group.

Table 90-2 Configure Host Protection Group

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Create host protection group	<b>host-guard group <i>group-name</i></b>	Mandatory By default, no host protection group is created.
Configure host protection group rules	<b>permit host <i>ip-address</i></b>	Mandatory

Step	Command	Description
		By default, the host protection group rules are not configured.

## Note

- Each host protection can support 128 rules at most.

### Configure Application of Host Protection Group

Apply the host protection group to the port to monitor the ARP packets received and protect the ARP table.

Table 90 Configuring Application of Host Protection Group

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Configure Application of Host Protection Group	<b>host-guard binding</b> <i>group-name</i>	Mandatory  By default, there is no host protection group applied on the port or aggregation group.

## 90.2.2 Host Guard Monitoring and Maintaining

Table 90 Host Guard Monitoring and Maintaining

Command	Description
<b>show host-guard binding</b> [ <b>interface</b> <i>interface-id</i>   <b>link-aggregation</b> <i>link-aggregation-id</i> ]	Show the application information of host protection group
<b>show host-guard group</b> [ <i>group-name</i> ]	Show the configuration information of host protection group and its rules

# 91 AAA

---

## 91.1 Overview

AAA means Authentication, Authorization, and Accounting. Since the birth of network, Authentication, Authorization and Accounting system has become the foundation of its operation. The use of various resources in the network needs to be managed by Authentication, Authorization and Accounting. Generally, AAA adopts the client/server structure. The client is running on NAS (Network Access Server), and the server is used for centralized management of user information. NAS is a server for users and a client for the server.

In particular, Authentication means to confirm the identity of users when they use the resources in the network system. During this process, the identity information obtained through interaction with users is submitted to the authentication server; the latter checks the identity information with the user information in the database, and then confirm whether users' identities are correct according to the processing result. Authorization means the network system authorizes users to use its resources in a specific way. This process specifies the services and permissions that the authenticated user can use and own after accessing the network, such as the IP address assigned. Accounting means the network system collects and records users' use of the network resources so as to charge fees from users for their use of the resources or use it for the purpose of auditing.

RADIUS (Remote Authentication Dial-In User Service) is a C/S-structured protocol. Its client was a NAS server at the beginning. RADIUS protocol authentication mechanism is flexible. It can use PAP, CHAP or Unix login. RADIUS is an extensible protocol, and all of its work is based on the vector of Attribute-Length-Value. The basic working principle of RADIUS is as follows: after users access the NAS, the NAS submits user information to the RADIUS server using data packet Access-Require, including user name, password and other related information. In particular, the user password is MD5 encrypted. The two parties use a shared key which is not propagated through network. The RADIUS server checks the legality of the user name and password, and when necessary, it can put forward a challenge to request further user authentication or similar authentication for the NAS. If it is legal, return the data packet Access-Accept to the NAS, allowing the user to proceed to the next step. Otherwise, it will return the data packet Access-Reject and deny user access. If the access is allowed, the NAS will request Account-Require to the RADIUS server which will give a response of Account-Accept prior to user statistics. At the same time, users can perform their own operations.

TACACS (Terminal Access Controller Access Control System) is an old authentication protocol for Unix network. It allows remote access server to send user login password to the authentication server which determines whether the user can log in to the system. As an encryption protocol, TACACS has a lower security than the later TACACS+ and RADIUS. In fact, TACACS+ is a new protocol. It has superseded previous protocols with RADIUS in existing network. TACACS+ uses Transmission Control Protocol (TCP), and RADIUS applies User Datagram Protocol (UDP). RADIUS combines authentication and authorization from the perspective of users, while TACACS+ separates them.

## 91.2 AAA Function Configuration

Table 91-1 AAA Function Configuration List

Configuration Task	
Configure AAA Domain	Configure ISP Domain
Configure Authentication Function under AAA Domain	Configure Default, Login and Dot1x Authentication Method under ISP Domain
Configure Authorization Function under AAA Domain	Configure Default, Login and Commands Authorization Method under ISP Domain
Configure Accounting Function under AAA Domain	Configure Default, Login, Dot1x and Commands Accounting Method under ISP Domain
Configure Authentication Method of Entering Privileged Mode	Configure Authentication Method of Entering Privileged Mode
Configure to Enable Command Line Authorization	Configure to Use Command Line Authorization
	Configure to Use Console Authorization
Configure System Accounting Function	Configure System Event Accounting Method
Configure Statistics-related Properties	Configure to Close Accounting of Empty User Name
	Configure Sending of Accounting Update Packet
	Configure Method of Sending Accounting Failure for Processing
Configure RADIUS Program	Configure RADIUS Server
	Configure RADIUS-related Properties

Configuration Task	
	Configure to Send Source Address of RADIUS Packet
Configure TACACS Program	Configure TACACS Server
	Configure to Send Source Address of TACACS Packet

### 91.2.1 Configure AAA Domain

**Domain:** NAS manages users based on ISP (Internet Service Provider) domain. Each user belongs to an ISP domain. Generally, the ISP domain to which the user belongs is determined by the user name provided by the user at the time of login. By default, the system has a system domain. You can configure the authentication, authorization and charging method of each type of access user under the domain.

The solution for user and AAA management based on domain is described as follows:

NAS device manages users based on ISP domain. Generally, the ISP domain to which the user belongs is determined by the user name provided by the user at the time of login.

"User name input by user" = "user name understood by user" + "domain name"

During user authentication, the device identifies its domain by the following order, and then performs the AAA policy in the domain:

- 1) [Optional] Log in/access the authentication domain specified by module configuration;
- 2) ISP domain specified in the user name;
- 3) Default ISP domain of the system.

#### Configuration Condition

None

#### Configure ISP Domain

Table 91-2 Configuring AAA Domain

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Enter the view of ISP domain	<b>domain</b> <i>isp-name</i>	Optional. By default, the system has an ISP domain named system.
Exit the global configuration mode	<b>exit</b>	-
Configure the default ISP domain	<b>domain default enable</b> <i>isp-name</i>	Optional. By default, the default ISP domain of the system is system domain.

### 91.2.2 Configure Authentication Function under AAA Domain

AAA provides a series of authentication method to guarantee the security of device and network service. For example, prohibit illegal users from operating the device by authenticating user login; authenticate users' entering into the privileged mode and limit users' permission of using the device; authenticate PPP session connection and limit the establishment of illegal connection.

#### Configuration Condition

None

#### Configure the Authentication Method Under ISP Domain

When a user try to log in to a specific ISP domain, AAA can authenticate this user and prohibit the user from logging in to the ISP domain if it fails to pass the authentication.

Table 91 Configuring List of Authentication Methods under ISP Domain

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the view of ISP domain	<b>domain</b> <i>isp-name</i>	Mandatory. By default, the system has an ISP domain named system.

Step	Command	Description
Configure the default authentication method under ISP domain	<b>aaa authentication default { none / local / radius-group <i>group-name</i> / tacacs-group <i>group-name</i> }</b>	Optional. By default, the default authentication method under ISP domain is local.
Configure the user login authentication method under ISP domain	<b>aaa authentication login { none / enable / local / radius-group <i>group-name</i> / tacacs-group <i>group-name</i> }</b>	Optional. By default, the login authentication method is not configured. The default authentication method under the domain is used.
Configure the dot1x authentication method under ISP domain	<b>aaa authentication dot1x { none / local / radius-group <i>group-name</i> / tacacs -group <i>group-name</i> }</b>	Optional. By default, the dot1x authentication method is not configured. The default authentication method under the domain is used.

### 91.2.3 Configure Authorization Function Under AAA Domain

After the successful authentication, the authorization function of AAA can control the administrator's permission of using device resources and the access of users to network resources, limit the administrator's execution of unauthorized command, and limit the access of users to unauthorized network resources.

#### Configuration Condition

For the command line authorization under the configuration domain, please enable command line authorization first to enable that configured under the domain to take effect.

#### Configure the Authorization Method under ISP Domain

When a user executes an authorized item under a specific ISP domain, AAA can authorize this user, grant permissions to it, and prohibit it from executing the authorized item under the domain if it fails to pass the authorization.

Table 91 Configuring List of Authorization Methods under ISP Domain

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Enter the view of ISP domain	<b>domain</b> <i>isp-name</i>	Mandatory.  By default, the system has an ISP domain named system.
Configure the default authorization method under ISP domain	<b>aaa authorization default</b> { <b>if-authenticated</b> / <b>local</b> / <b>none</b> / <b>radius-group</b> <i>group-name</i> / <b>tacacs-group</b> <i>group-name</i> }	Optional.  By default, the authorization method under ISP domain is none.
Configure the authorization method of commands under ISP domain	<b>aaa authorization commands</b> <i>cmd-lvl</i> { <b>if-authenticated</b> / <b>none</b> / <b>radius-group</b> <i>group-name</i> / <b>tacacs-group</b> <i>group-name</i> }	Optional.  By default, the authorization method of commands under ISP domain is not configured. The authorization method under the domain is none.  To enable this configuration to take effect, you must enable the command authorization function.
Configure the user login authorization method under ISP domain	<b>aaa authorization login</b> { <b>if-authenticated</b> / <b>local</b> / <b>none</b> / <b>radius-group</b> <i>group-name</i> / <b>tacacs-group</b> <i>group-name</i> }	Optional.  By default, the login authorization method under ISP domain is not configured. The default authorization method under the domain is used.

---

 **Note**

- aaa authorization commands and aaa authorization config-commands can be configured in any order.
- 

### 91.2.4 Configure Accounting Function under AAA Domain

Users' use of commands on the device, login of sessions, network service conditions and system events can be summarized with the user-defined method. The result provides a basis for charging users.

#### Configuration Condition

None

#### Configure the Accounting Method Under ISP Domain

When a user successfully logs in to a certain ISP domain, AAA can account for this user, including start login time, end login time, and the commands input.

Table 91 Configuring Accounting Methods under ISP Domain

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the view of ISP domain	<b>domain</b> <i>isp-name</i>	Mandatory. By default, the system has an ISP domain named system.
Configure the accounting method of command lines under ISP domain	<b>aaa accounting commands</b> <i>cmd-lvl</i> { [ <b>broadcast</b> ] <b>tacacs-group</b> <i>group-name</i> }	Optional. By default, the command accounting method is not configured, and command accounting is not conducted.
Configure the default accounting	<b>aaa accounting default</b> { <b>none</b>   { <b>start-stop</b>   <b>stop-only</b>   <b>wait-start</b> [ <b>broadcast</b> ] }	Optional. By default, the accounting

Step	Command	Description
method under ISP domain	<b>{ radius-group group-name / tacacs-group group-name }}</b>	method under ISP domain is none.
Configure the user login accounting method under ISP domain	<b>aaa accounting login{ none   { start-stop   stop-only   wait-start [ broadcast ] { radius-group group-name / tacacs-group group-name } } }</b>	Optional. By default, the login accounting method under ISP domain is not configured. The default accounting method under ISP domain is used.
Configure the dot1x accounting method under ISP domain	<b>aaa accounting dot1x { none   { start-stop   stop-only   wait-start [ broadcast ] { radius-group group-name / tacacs-group group-name } } }</b>	Optional. By default, the dot1x accounting method under ISP domain is not configured. The default accounting method under ISP domain is used.

### 91.2.5 Configure the Authentication Method of Entering Privileged Mode

After the user successfully logs in to the device, AAA can input enable command for the user to enter the privileged mode for authentication and prohibit the user who fails to pass the authentication from entering the privileged mode.

#### Configuration Condition

None

#### Configure the Privileged Mode Authentication Method

Table 91 Configuring Privileged Mode Authentication Method

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the privileged mode	<b>aaa authentication enable-method { none / enable / radius-</b>	Optional.

Step	Command	Description
authentication method	<b>group</b> <i>group-name</i> / <b>tacacs-group</b> <i>group-name</i> }	By default, the privileged mode authentication method is enable.

---

### Note

- When using the RADIUS authentication method, the password of the user name in the format of \$enableLEVEL\$ is used as the authentication password. In particular, LEVEL means the user level entered by current user. Its value ranges from 0 to 15, with level 15 being the highest.
- 

## 91.2.6 Configure to Enable Command Line Authorization

### Configuration Condition

None

### Configure to Use Command Line Authorization

The device has commands with levels from 0 to 15. Command authorization is used to determine the level of command used by the user through the authorization method, and restrict the user from using the command higher than current level.

Table 91 Enabling Command Authorization in Global Mode

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable command line authorization	<b>aaa authorization config-commands</b>	Mandatory. By default, the command line authorization function is closed.

### Configure to Use CONSOLE Authorization

To restrict access to the CONSOLE port, you can enable CONSOLE port authorization and activate the command authorization function. After that, the device will authorize the commands executed by the CONSOLE port.

Table 91 Configuring to Use Console Authorization

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure to Use Console Authorization	<b>aaa authorization console</b>	Mandatory. By default, the Console authorization is disabled.

### 91.2.7 Configure the System Event Accounting Function

Users may send the events like system start and restart to the server for accounting by configuring the system event accounting method.

#### Configuration Condition

None

#### Configure System Event Accounting Method

Table 91 Configuring List of System Event Accounting Methods

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure System Event Accounting Method	<b>aaa accounting system { none   { start-stop [broadcast] { tacacs-group group-name } } }</b>	Mandatory By default, the accounting of system event is not conducted.

---

 **Note**

- System event account supports TACACS protocol instead of RADIUS protocol.
- 

## 91.2.8 Configure Statistics-related Properties

### Configuration Condition

None

### Configure to Close Accounting of Empty User Name

Users may close the AAA's accounting of empty user names by configuring the command **aaa accounting suppress null-username**. By default, AAA's accounting of empty user names is enabled.

Table 1 Configuring to Close Accounting of Empty User Names

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure to Close Accounting of Empty User Name	<b>aaa accounting suppress null-username</b>	Mandatory. By default, the accounting of empty user names is enabled.

### Configure Sending of Accounting Update Packet

Users can configure the method of sending accounting update packets, including real-time sending and periodic sending.

Table 91 Configuring Sending of Accounting Update Packets

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Configure Sending of Accounting Update Packet	<b>aaa accounting update periodic interval</b>	Mandatory.  By default, the accounting update packets are not sent.

### Configure Method of Sending Accounting Failure for Processing

Table 91 Configuring Method of Sending Accounting Failure for Processing

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the method of sending accounting failure for processing	<b>aaa accounting start-fail {online   offline}</b>	Optional.  By default, users who fail to start the accounting cannot go online.

### 91.2.9 Configure RADIUS Program

To configure RADIUS program, you must first configure key parameters of the server.

#### Configuration Condition

None

#### Configure RADIUS Server

If AAA needs to use RADIUS for authentication, authorization and accounting, you are required to configure RADIUS server-related parameters, including server IP address, authentication/authorization port, accounting port, and shared key.

Before entering the RADIUS server, you need to configure a RADIUS server group. When quoting the server group name to configure the method list, you can use the RADIUS server group for authentication, authorization and accounting of users.

Table 2 Configuring RADIUS Server

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the RADIUS server group name (this command can also lead to the RADIUS server group configuration mode)	<b>aaa server group radius <i>group-name</i></b>	Mandatory. By default, the RADIUS server group name is not configured.
Configure RADIUS Server	<b>server {<i>ip-address</i> <i>ipv6 ip-address</i>} [ <b>acc-port</b> <i>acc-port-num</i> ] [ <b>auth-port</b> <i>auth-port-num</i> ] [ <b>priority</b> <i>priority</i> ] { <b>key</b> [ <b>0</b>   <b>7</b> ] <i>key</i> }</b>	Mandatory. By default, the RADIUS server is not configured.
Configure quiet period of RADIUS	<b>dead-time <i>dead-time</i></b>	Optional. By default, the quiet period of RADIUS server is 0, i.e. no quiet period.
Configure the maximum times of RADIUS retransmission	<b>retransmit <i>retries</i></b>	Optional. By default, the maximum times of retransmission by RADIUS server are 3.
Configure the response timeout time of RADIUS server	<b>timeout <i>timeout</i></b>	Optional. By default, the timeout time of waiting for the RADIUS server to respond is 5 seconds.
Configure not to check the TAG tag when resolving the tunnel attributes	<b>tunnel without-tag</b>	Optional. By default, TAG tag is required when resolving the tunnel attributes

Step	Command	Description
issued by the RADIUS server		issued by the RADIUS server
Configure the VRF to which the RADIUS server group belongs	<b>ip vrf forwarding</b> <i>vrf-name</i>	Optional. By default, the RADIUS server group belongs to the global VRF.

### Note

- The device selects the order of using the **RADIUS** server according to the **priority** value configured.
- Quiet period means that the device marks the **RADIUS** servers which give no response to the authentication request unavailable, and no longer gives request to these servers during the **dead time**.
- The shared keys configured on the device and the **RADIUS** server must be consistent.

## Configure RADIUS-related Properties

Table 91 Configuring Relevant Attributes of RADIUS

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the value of service-type in the RADIUS packets for login authentication	<b>radius login service-type</b> <i>attr-value</i>	Optional By default, the value of service-type in RADIUS packet is 7.
Configure the maximum number of concurrent packets of NAS device and RADIUS server	<b>radius control-speed</b> <i>pck-num</i>	Optional By default, the maximum number of concurrent packets of NAS

Step	Command	Description
		device and RADIUS server is 100.

### Configure to Send Source Address of RADIUS Packet

Table 91 Configuring Source Address of Sending RADIUS Packets

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the interface selected by the RADIUS source address	<b>ip radius source-interface</b> <i>interface-name</i> [ <b>vrf</b> <i>vrf-name</i> ]	Optional By default, the device automatically selects source interface.

### Configure the Accounting-on Function Which Can Send RADIUS

The accounting-on function is mainly used to make all the online users on the specified RADIUS server offline when the AAA process is pulled up for the first time. By default, the accounting-on function is disabled; when the account-on function is enabled, the default retransmission interval is 6 seconds, and the maximum times of retransmission are 50; since the SPU of high-end device starts slow, it is recommended that the retransmission times and interval be no less than the default values.

Table 3 Configuring Accounting-on Function of RADIUS

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the RADIUS server group mode	<b>aaa server group radius</b> <i>group-name</i>	-
Configure the accounting-on function of RADIUS	<b>accounting-on enable</b> [ <i>interval seconds</i>   <b>send</b> <i>send-times</i> ]	Optional.

Step	Command	Description
		By default, the accounting-on function is disabled.

## 91.2.10 Configure TACACS Program

To configure TACACS program, you must first configure key parameters of the server.

### Configuration Condition

None

### Configure TACACS Server

After the TACACS server is configured, if AAA needs to use TACACS for authentication, authorization and accounting, you are required to configure TACACS server-related parameters, including server IP address, shared key, and server port number.

When quoting the server group name to configure the method, you can use the TACACS server group for authentication, authorization and accounting of users.

Table 4 Configuring TACACS Server

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the TACACS server group name (this command can also lead to the TACACS server group configuration mode)	<b>aaa server group tacacs <i>group-name</i></b>	Mandatory. By default, the TACACS server group name is not configured.
Configure TACACS Server	<b>server {<i>ip-address</i>   ipv6 <i>ip-address</i>} [ port <i>port-num</i> ] [ priority <i>priority</i> ] { key [ 0   7 ] <i>key</i>}</b>	Mandatory. By default, the member server of TACACS server group is not configured.

Step	Command	Description
Configure the response timeout time of TACACS server	<b>timeout</b> <i>timeout</i>	Optional. By default, the timeout time of waiting for the TACACS server to respond is 5 seconds.
Configure the VRF attribute of TACACS server group	<b>ip vrf forwarding</b> <i>vrf-name</i>	Optional. By default, the TACACS server group belongs to the global VRF.

### Note

- You can execute `server {ip-address|ipv6 ip-address} [port port-num] [priority priority] {key [0 | 7] key}` multiple times to configure the multiple TACACS servers under the TACACS server group. The device will select servers by the configuring order for authentication. When a server fails, the device will automatically select the next one.
- The shared keys configured on the device and the TACACS server must be consistent.

### Configure to Send Source Address of TACACS Packet

Table 91 Configuring Source Address of Sending TACACS Packets

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the interface selected by the TACACS source address	<b>ip tacacs source-interface</b> <i>interface-name</i> [ <b>vrf</b> <i>vrf-name</i> ]	Optional. By default, the device automatically selects source interface.

## 91.2.11AAA Monitoring and Maintaining

Table 5 AAA Monitoring and Maintaining

Command	Description
<b>debug aaa { authentication   authorization   accounting   event   error   all }</b>	Turn on the AAA debugging information switch
<b>debug radius [details]</b>	Turn on the TACACS debugging information switch
<b>debug tacacs</b>	Turn on the TACACS debugging information switch
<b>show aaa configuration</b>	Show the information of AAA configuration
<b>show aaa module [dot1x   shell   shell-cmd   shell-web ]</b>	Show the function module of AAA and the result of operating AAA last time by this module
<b>show aaa server [ radius   tacacs ]</b>	Show the RADIUS/TACACS server configuration and status of AAA
<b>show aaa session [dot1x   shell   shell-web ]</b>	Show AAA statistics session
<b>show aaa source-address</b>	Show the source address used by AAA

## 91.3 Typical Configuration Example of AAA

### 91.3.1 Configure Telnet User Login for Local Authentication

#### Network Requirements

- Enable the Device to conduct local authentication for Telnet user login

#### Network Topology



Figure 91 Network Topology for Configuring Local Authentication for Telnet User Login

### Configuration Steps

Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configure IP addresses for the ports. (Omitted)

Step 3: Configure the Device.

#Configure both user name and password as admin1.

```
Device#configure terminal
Device(config)#local-user admin1 class manager
Device(config-user-manager-admin1)#service-type telnet
Device(config-user-manager-admin1)#password 0 admin1
Device(config-user-manager-admin1)#exit
```

#Configure the AAA authentication mode to local authentication.

```
Device(config)#domain system
Device(config-isp-system)#aaa authentication login local
Device(config-isp-system)#exit
```

#Configure Telnet session and enable AAA local authentication.

```
Device(config)#line vty 0 15
Device(config-line)#login aaa
Device(config-line)#exit
```

Step 4: Check the result.

When the client logs in to the Device through telnet, it can successfully go to the Shell user interface of the Device by inputting user name and password admin1.

## 91.3.2 Configure Telnet User Login for RADIUS Authentication, Authorization and Accounting

### Network Requirements

- The Device is connected to the Telnet client and RADIUS server, and the IP route is reachable.
- The IP address of the RADIUS server is 2.0.0.2/24; the authentication and authorization port is 1812; the accounting port is 1813; the shared key is admin.
- When the Telnet user logs in to the Device, it needs to perform authentication, authorization, and accounting through the RADIUS server.

- When the RADIUS server fails, local authentication and authorization apply.

### Network Topology

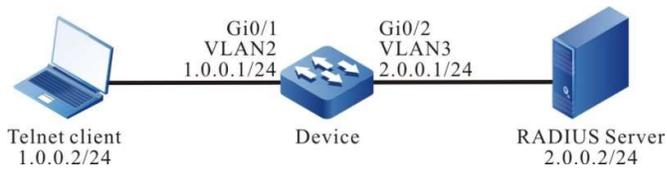


Figure 911 Network Topology for Configuring RADIUS Authentication, Authorization and Accounting for Telnet User Login

### Configuration Steps

- Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)
- Step 2: Configure IP addresses for the ports. (Omitted)
- Step 3: Configure the Device.

#Configure AAA to use RADIUS authentication/authorization and accounting.

---

#### Note

- For authentication and authorization, first use the first method in the list of methods, and use the second method when the server fails.
- 

```

Device#configure terminal
Device(config)#domain system
Device(config-isp-system)#aaa authentication login radius-group radius-group local
Device(config-isp-system)#aaa authorization login radius-group radius-group local
Device(config-isp-system)#aaa accounting login start-stop radius-group radius-group
Device(config-isp-system)#exit
  
```

#Configure the RADIUS server: the authentication port is 1812; the accounting port is 1813; the shared key is admin.

```

Device(config)#aaa server group radius radius-group
Device(config-sg-radius-radius-group)#server 2.0.0.2 auth-port 1812 acct-port 1813 key admin
Device(config-sg-radius-radius-group)#exit
  
```

#Configure Telnet session and enable RADIUS authentication, authorization and accounting.

```

Device(config)#line vty 0 15
Device(config-line)#login aaa
Device(config-line)#exit
  
```

- Step 4: Configure the RADIUS server.

For the interface setting of RADIUS server, please see the help document of the server. The specific steps are shown below.

#Add user admin on the RADIUS server, set the password as admin, and configure the user level as 15.

#Set the IP address of the server as 2.0.0.2, shared key as admin, authentication port as 1812, and accounting port as 1813.

#Set the IP address of the client as 2.0.0.1 and shared key as admin.

Step 5: #Check the result, and verify authentication, authorization and accounting.

#After the Telnet user logs into the Device for successful authorization, show privilege to view the user priority, i.e. 15.

#Check the login and disconnection information on the RADIUS server.

### 91.3.3 Configure Telnet User Level Switch for RADIUS Authentication

#### Network Requirements

- The Device is connected to the Telnet client and RADIUS server, and the IP route is reachable.
- The IP address of the RADIUS server is 2.0.0.2/24; the authentication/authorization port is 1812; the shared key is admin.
- When the Telnet user logs in to the Device and the user level switches to 3 from 1, it needs to perform authentication through the RADIUS server.

#### Network Topology

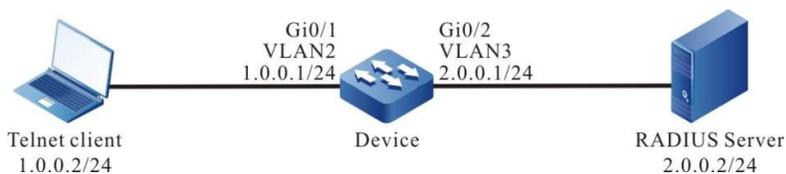


Figure 91 Network Topology for Configuring RADIUS Authentication for Telnet User Level Switch

#### Configuration Steps

Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configure IP addresses for the ports. (Omitted)

Step 3: Configure the Device.

#Configure user level switch for RADIUS authentication.

```
Device#configure terminal
Device(config)#aaa authentication enable-method radius-group radius-group
Device(config)#domain system
Device(config-isp-system)#aaa authentication login radius-group radius-group local
```

```
Device(config-isp-system)#exit
```

#Configure the RADIUS server: the authentication port is 1812; the shared key is admin.

```
Device(config)#aaa server group radius radius-group
Device(config-sg-radius-radius-group)#server 2.0.0.2 auth-port 1812 acct-port 1813 key admin
Device(config-sg-radius-radius-group)#exit
Device(config)#line vty 0 15
Device(config-line)#login aaa
Device(config-line)#exit
```

Step 4: Configure the RADIUS server.

For the interface setting of RADIUS server, please see the help document of the server. The specific steps are shown below.

#Add user name \$enab3\$ (user level 3), and set the password as admin.

---

### Note

- User level switch uses the user name authentication in the format of \$enabLEVEL\$. In particular, the uppercase LEVEL is the level to which the user intends to switch.
  - No authentication is required when the user level decreases.
- 

Step 5: Check the result.

Telnet users input user name and password according to the prompt. After login, the user level is 1 by default. After executing the command enable 3, input the password admin. After successful authentication by the RADIUS server, the user level switches to 3.

## 91.3.4 Configure TACACS Authorization and Accounting of SHELL Command

### Network Requirements

- Device and TACACS server are interconnected, and the route is reachable.
- The IP address of the TACACS server is 2.0.0.2/24; the service port is 49; the shared key is admin.
- After the Telnet client logs in to the Device, the SHELL command with a user level of 15 is required to be authorized by the TACACS server and recorded on the TACACS server.

### Network Topology

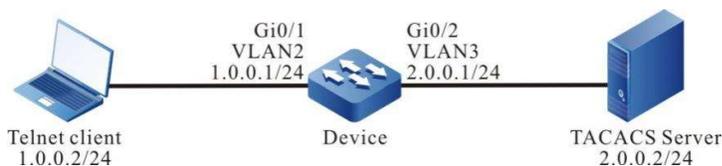


Figure 91 Network Topology for Configuring TACACS Authorization and Accounting for SHELL Command

### Configuration Steps

Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configure IP addresses for the ports. (Omitted)

Step 3: Configure the Device.

#Configure authorization and accounting of TACACS command.

---

 **Note**

- The authentication must succeed prior to authorization and accounting.
- 

```
Device#configure terminal
Device(config)#domain system
Device(config-isp-system)#aaa authentication login tacacs-group tacacs-group local
Device(config-isp-system)#aaa authorization commands 15 tacacs-group tacacs-group
Device(config-isp-system)#aaa accounting commands 15 tacacs-group tacacs-group
Device(config-isp-system)#exit
Device(config)#aaa authorization config-commands
```

#Configure the TACACS server: the service port is 49; the shared key is admin.

```
Device(config)#aaa server group tacacs tacacs-group
Device(config-sg-tacacs-tacacs-group)#server 2.0.0.2 port 49 key admin
Device(config-sg-tacacs-tacacs-group)#exit
```

#Configure Telnet session and enable TACACS authorization and accounting.

```
Device(config)#line vty 0 15
Device(config-line)#login aaa
Device(config-line)#exit
```

Step 4: Configure TACACS server.

For the interface setting of TACACS server, please see the help document of the server. The specific steps are shown below.

#Add the client 2.0.0.1 on the server; the shared key is admin; select "TACACS+(Cisco IOS)" authentication.

#Set SHELL command authorization for the admin of Telnet user. Permit commands configure terminal, router ospf and router rip, and deny other commands.

Step 5: Check the result.

#After logging in to the Device, the Telnet user can execute corresponding SHELL command. The command which is successfully authorized can be successfully executed, while the command which fails to be authorized cannot be executed.

```
Device#configure terminal
% Enter configuration commands, one per line. End with CNTL+Z.
Device(config)#router ospf 100
Device(config-ospf)#exit
Device(config)#router rip
Device(config-rip)#exit
Device(config)#interface gigabitethernet 0/1
Command authorization failed
Device(config)#router bgp 100
Command authorization failed
```

#View the statistics of SHELL command.

#Check the statistics of SHELL command on the TACACS server.



# 92 802.1X

---

## 92.1 Overview

### 92.1.1 802.1X

802.1X is a broadband access authentication program proposed by IEEE in June 2001. It defines a Port-Based Network Access Control protocol. By utilizing the physical access features of IEEE 802 architecture LAN, 802.1X provides the method of connecting the device on LAN port in point-to-point mode for authentication, charging and authorization.

802.1X system is a typical client/server structure, as shown in the figure below. It includes three entities, i.e. Supplicant system, Authentication system, and Authentication server system.



Figure 92 802.1X System Structure

- Install software that supports 802.1X authentication on the client and sends an authentication request to the authentication device. After the authentication succeeds, it can normally access the network.
- Located between the client and the authentication server, the authentication device controls network access of the client through server interaction.
- Generally, the authentication server is RADIUS (Remote Authentication Dial-In User

Service) server. It is used to verify the legality of the client and notify the authentication result to the authentication device which controls network access of the client according to the authentication result.

The EAP (Extensible Authentication Protocol) used in 802.1X authentication is a general protocol for PPP authentication. It is used to realize the interaction of authentication information between the client, authentication device, and authentication server. The 802.1X protocol uses the EAPOL (EAP Over LAN) frame encapsulation format to encapsulate EAP packets to realize the interaction between client and authentication device. Depending on the application scenarios, the 802.1X protocol will encapsulate EAP packets in different frame formats to realize the interaction between authentication device and authentication server. In relay authentication, the EAP packets are encapsulated in EAPOR (EAP Over RADIUS) frame format; in termination authentication, EAP packets are encapsulated in standard RADIUS frame format.

802.1X authentication has two types, i.e. relay and termination.

The following figure shows relay authentication mode:

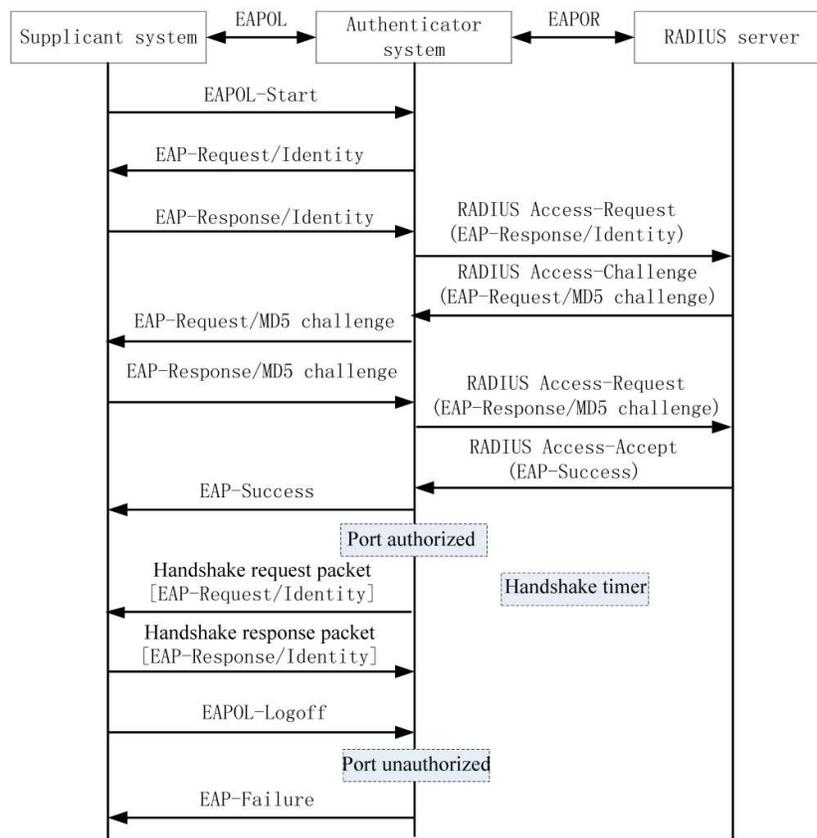


Figure 92 802.1X Relay Authentication Process

The relay authentication process is as follows:

- When the users intend to access the network, they can open the program on the 802.1X client, input the legal user name registered on the authentication server and password,

and initiate an authentication request (EAPOL-Start packet). At this time, the client program will send the packet requesting authentication to the authentication device, and start an authentication process;

- After the authentication device receives the data frame of requesting authentication, it will send a user name which the request frame (EAP-Request/Identity packet) requires the client program of the user to send;
- The client program responds to the request sent by the authentication device and sends the user name to the authentication device through a data frame (EAP-Response/Identity packet). The authentication device encapsulates the data frame sent by the client in a packet (RADIUS Access-Request packet) and sends it to the authentication server for processing;
- After the RADIUS server receives the user name forwarded by the authentication device, it compares the information with the user name table in the database, finds the password corresponding to the user name, encrypts it with an encrypted character randomly generated, and sends this character through the RADIUS Access-Challenge packet to the authentication device which then forwards it to the client program;
- After the client program receives the encrypted character (EAP-Request/MD5 Challenge packet) from the authentication device, it uses the encrypted character to encrypt the password part (this kind of encryption algorithm is usually irreversible, and it will generate EAP-Response/MD5 Challenge packet), and passes it to the authentication server through the authentication device;
- The RADIUS authentication server compares the encrypted password received (RADIUS Access-Request packet) with the local password after encryption operation. If they are the same, it is believed that this user is legal and it will give the message that authentication succeeds (RADIUS Access-Accept packet and EAP-Success packet);
- The authentication device changes the port to authorized after receiving the message that authentication succeeds, allowing the user to access the network through the port;
- The client can also send an EAPOL-Logoff packet to the authentication device to request to go offline. The authentication device changes the port status from authorized to unauthorized, and sends an EAP-Failure packet to the client.

This requires both the authentication device and the authentication server support EAP.

The following figure shows termination authentication mode:

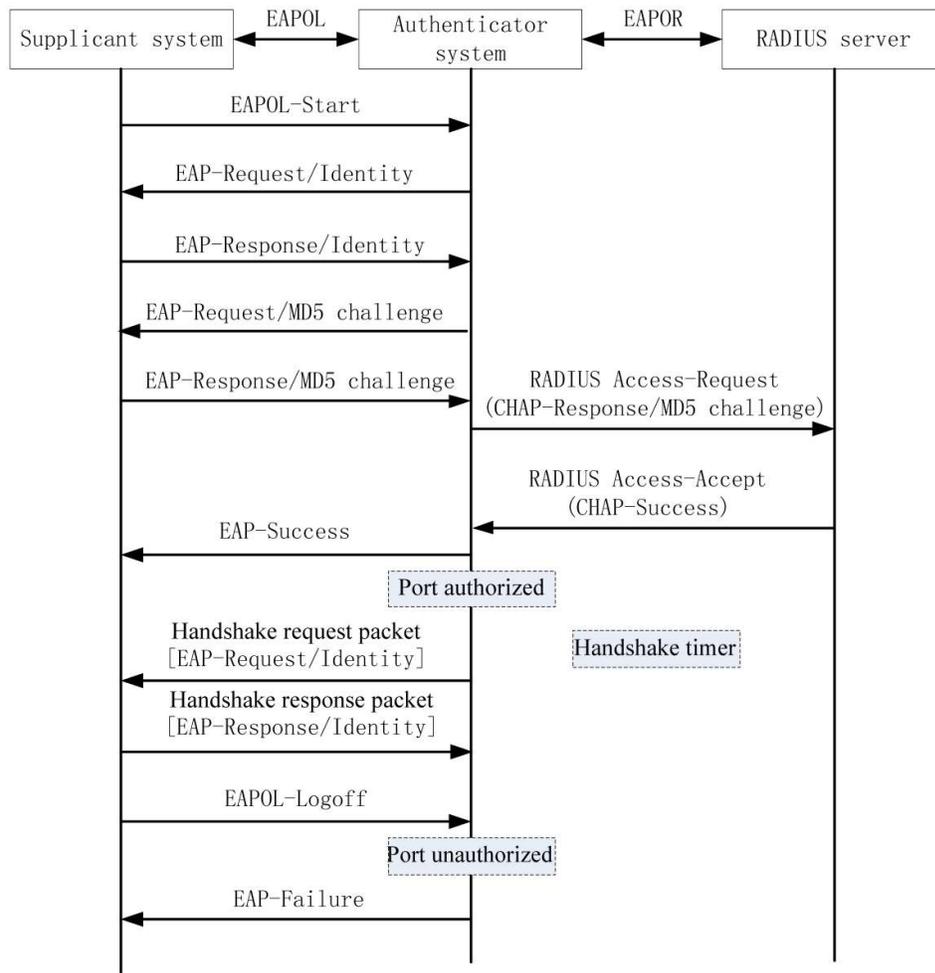


Figure 92802.1X Termination Authentication Process

- The process of termination authentication is different from that of relay authentication in that the randomly encrypted character for encryption of user password is generated by the authentication device which then sends the user name, randomly encrypted character and client encryption password to the RADIUS server for relevant authentication processing.

Termination authentication is used for the authentication server which is deployed earlier and doesn't support EAP protocol.

The authentication device supports two types of access control:

- Port-based access control: After the first user under the port is successfully authenticated, other users can access the network without authentication. But when the first user goes offline, other users are not allowed to access the network;
- Macbased access control: All access users under the port need to be individually authenticated. After a user goes offline, it cannot access the network any longer. Yet this

does not affect other users' access to the network.

Sometimes Auto VLAN is also called Assigned VLAN. When the client passes the server authentication, the server will send the authorized VLAN information to the authentication device. If this VLAN exists and is legal in the authentication device, the authentication port will be added to it. After the client goes offline, the port becomes unauthenticated again and is deleted from this Auto VLAN, and the default VLAN of the port recovers to the previous one.

When the Guest VLAN function is enabled, the user can only access the resources in the VLAN without authentication; after the successful user authentication, the port leaves the Guest VLAN and the user can access other network resources. Generally, the user can obtain 802.1X client software from the Guest VLAN to upgrade the client, or execute other application (e.g. anti-virus software and OS patches) upgrading. After enabling 802.1X authentication and correctly configuring the Guest VLAN, the port will be added to the Guest VLAN in Untagged mode. At this time, the user under the port in the Guest VLAN initiates authentication. If the authentication fails, the port is still in the Guest VLAN; if it succeeds, one of the following two circumstances applies:

- If the authentication server issues a VLAN, the port moves from the Guest VLAN to the issued VLAN. After the user goes offline, the port will go back to the Guest VLAN;
- If the authentication server does not issue any VLAN, the port moves from the Guest VLAN to the Config VLAN that has been configured in the authentication device. After the user goes offline, the port will go back to the Guest VLAN.

### 92.1.2 Secure Channel Authentication

The secure channel authentication function is based on the 802.1X authentication function. In addition to 802.1X authentication, it can open a secure channel for specific terminal users so that they can access the resources in the specified network when they are not authenticated, or specify specific terminal users to access network resources without authentication.

### 92.1.3 MAC Address Authentication

In the actual network, in addition to plenty of terminal users, there may be some network terminals (e.g. network printers). These terminals do not have their own or cannot be installed with 802.1X authentication client software. In this case, you can access the network without client authentication. With this authentication method, users don't have to install any 802.1X authentication client software. After detecting the MAC address of the user for the first time, the authentication device sends the configured user name and password or the MAC address of the user as user name and password to the authentication server for authentication.

Generally, the MAC address uses the following two formats of user name and password:

MAC address: Use the MAC address of the authenticated user as user name and password;

Fixed user name and password: Use the user name and password that have been configured on the authentication device.

## 92.2 802.1X Function Configuration

Table 92-1 802.1X Function Configuration List

Configuration Task	
Configure 802.1X Authentication	Enable 802.1X Authentication
Configure Secure Channel Authentication	Enable Secure Channel Authentication Function
	Configure and Apply Secure Channel
Configure 802.1X Authentication and Secure Channel Authentication Attributes	Configure Port Authentication Method
	Configure Multicast Trigger
	Configure Reauthentication Function
	Configure the Maximum Number of Port Authentication Failures
	Configure Function of Omitting IP Field in User Name
	Configure Function of Transparent Transmission of Packets
	Configure Keepalive Function
	Configure Function of Not Waiting for Response of Server
Configure MAC Address Authentication	Enable MAC Address Authentication Function
	Configure MAC Address Authentication User Name Format
	Configure Domain Name Used in Global MAC Authentication
Configure Common Attributes	Configure Control Direction

## Configuration Task

Configure Authenticable Host List
Configure IP Authorization Function
Configure the Maximum Times of Transmitting Authentication Request Packets
Configure the Maximum Times of Transmitting Authentication Packets
Configure Function of Data Logging
Configure ARP Keepalive Function
Configure the Maximum Number of Users on Port
Configure IP ACL Prefix Name
Configure Default Valid VLAN
Configure Function of Permitting Unauthenticated Users to Communicate in the VLAN of PVID
Configure Port Access Control Method
Configure Guest VLAN
Configure Guest ACL
Configure Critical VLAN
Configure User Authentication Migration Function
Configure Timer Parameters
Restore Default Configurations of Port
Configure Step Size of Log Record

## 92.2.1 Configure 802.1X Authentication Function

Permit to configure both 802.1X authentication and MAC address authentication under the same port.

- When MAC address authentication is first conducted for terminal users, if the authentication succeeds, the 802.1X authentication initiated by these terminal users will not be processed. Otherwise, the 802.1X authentication initiated by these terminal users will be processed.
- If 802.1X authentication is first conducted for the terminal users, no MAC address authentication is required.

### Configuration Condition

None

### Enable 802.1X Authentication

To enable the 802.1X authentication function, the terminal user has to install the client software with 802.1X authentication.

Table 92-2 Enabling 802.1X

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable global 802.1X authentication	<b>dot1x { enable   disable }</b>	Optional By default, the global 802.1X authentication function is enabled.
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected. After you enter the layer-2
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.

Step	Command	Description
Enable 802.1X Authentication	<b>dot1x port-control { enable   disable }</b>	Mandatory  By default, the 802.1X authentication function under the port is disabled.

## Note

- The 802.1X authentication and secure channel authentication functions cannot be both enabled under the same port.
- The 802.1X authentication and port security functions can be both enabled under the same port, but port security IP rules and MAX rules are not allowed to configure.
- When both 802.1X authentication and port security functions are used, if the port security is configured with relevant MAC rules, 802.1X doesn't process the sending packets and authentication request of this terminal. Instead, they will be processed by port security.

### Configure the Function of Triggering the Generation of 802.1X Users Through ARP/IP Packets

After the 802.1X authentication function is enabled under the port, if the terminal user intends to view its information on the authentication device when it does not initiate authentication, you need to configure function of triggering the generation of 802.1X users through ARP/IP packets.

If the functions of 802.1X authentication and triggering the generation of 802.1X users through ARP/IP packets are both enabled under the same port, when the authentication device receives the ARP or IP packets of the terminal user under the port, 802.1X user can be generated.

Table 92-3 Enabling Function of Triggering Generation of 802.1X Users Through ARP/IP Packets

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2 Ethernet interface
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	configuration mode, the subsequent configuration

Step	Command	Description
		takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Configure the function of triggering the generation of 802.1X users through ARP/IP packets	<b>dot1x arp-ip-auth { enable   disable }</b>	Mandatory  By default, the function of triggering the generation of 802.1X users through ARP/IP packets under the port is disabled.
Configure the timeout value of triggering the generation of 802.1X users through ARP/IP packets	<b>dot1x arp-ip-auth timeout <i>timeout-value</i></b>	Optional  By default, the timeout value of triggering the generation of 802.1X users through ARP/IP packets under the port is 5 minutes.

## 92.2.2 Configure Secure Channel Authentication

### Configuration Condition

None

### Enable Secure Channel Authentication

The secure channel authentication function is based on the 802.1X authentication function. In addition to 802.1X authentication, it can open a secure channel for specific terminal users so that they can access the resources in the specified network when they are not authenticated, or specify specific terminal users to access network resources without authentication.

Table 92-4 Enabling Secure Channel Authentication

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enable secure channel authentication	<b>dot1x free-ip</b>	Mandatory  By default, the secure channel authentication function under the port is disabled.

---

### Note

The secure channel authentication and port security functions cannot be both enabled under the same port.

The 802.1X authentication and secure channel authentication functions cannot be both enabled under the same port.

The MAC address authentication and secure channel authentication functions cannot be both enabled under the same port.

When the secure channel authentication function is enabled under the port, yet no secure channel is applied or no secure channel rule is configured, the secure channel authentication function is the same as 802.1X authentication function.

In case of secure channel authentication, after the user passes the authentication, it will occupy chip resources. Insufficient chip resources will lead to failure of user authentication.

---

After enabling the secure channel authentication function under the port, to permit terminal users to access the resources in the specified network when they are not authenticated, or specify specific terminal users to access network resources without authentication, you need to configure and apply secure channel.

Secure channel rules can be configured as follows.

- Permit terminal users to access specified network resources.
- Permit specified terminal users to access network resources.

Table 92 Applying Secure Channel

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure secure channel	<b>hybrid access-list advanced</b> { <i>access-list-number</i>   <i>access-list-name</i> }	Mandatory  By default, no secure channel is configured in the device.
Configure secure channel rules	[ <i>sequence</i> ] <b>permit [ether-ipv6] protocol</b> { <b>any</b>   <i>source-ip-addr source-wildcard</i>   <b>host</b> <i>source-ip-addr</i> } { <b>any</b>   <i>source-mac-addr source-wildcard</i>   <b>host</b> <i>source-mac-addr</i> } { <b>any</b>   <i>destination-ip-addr destination-wildcard</i>   <b>host</b> <i>destination-ip-addr</i> } { <b>any</b>   <i>destination-mac-addr destination-wildcard</i>   <b>host</b> <i>destination-mac-addr</i> }	Mandatory  By default, there are no secure channel rules under the secure channel.
Apply secure channel	<b>global security access-group</b> { <i>access-group-number</i>   <i>access-group-name</i> }	Mandatory  By default, no secure channel is applied in the system.



**Note**

A device can be configured with multiple secure channels, and a secure channel may have multiple secure channel rules.

The type of secure channel can be mixed advanced ACL only, and only one secure channel can be applied in the device.

### Configure the Function of URL Redirection

When URL redirection is configured on the authentication device, the authentication device will redirect the URL address the user visits to the configured redirected URL address when the user accesses a non-authentication-free network segment where it is not authenticated or fails to pass the authentication. In the specified URL page, users can download/upgrade the authentication client, or update software.

Table 92 Configuring URL Redirection Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure secure channel	<b>hybrid access-list advanced</b> { <i>access-list-number</i>   <i>access-list-name</i> }	Mandatory  By default, no secure channel is configured in the device.
Configure secure channel rules	[ <i>sequence</i> ] <b>permit [ether-ipv6] protocol</b> { <b>any</b>   <i>source-ip-addr source-wildcard</i>   <b>host</b> <i>source-ip-addr</i> } { <b>any</b>   <i>source-mac-addr source-wildcard</i>   <b>host</b> <i>source-mac-addr</i> } { <b>any</b>   <i>destination-ip-addr destination-wildcard</i>   <b>host</b> <i>destination-ip-addr</i> } { <b>any</b>   <i>destination-mac-addr destination-wildcard</i>   <b>host</b> <i>destination-mac-addr</i> }	Mandatory  By default, there are no secure channel rules under the secure channel.
Apply secure channel	<b>global security access-group</b> { <i>access-group-number</i>   <i>access-group-name</i> }	Mandatory  By default, no secure channel is applied in the system.

Step	Command	Description
Configure the function of URL redirection	<b>dot1x url <i>url-redirect-string</i></b>	Mandatory  By default, redirected URL address is not configured on the device.

---

### Note

The authentication-free network segment should have the IP address of DNS server and the IP address of redirected URL link.

The client is required to apply for an address from the DHCP server. When the authentication device itself is not a DHCP server, the DHCP RELAY function should be enabled to ensure that the client can normally obtain IP address.

---

### 92.2.3 Configure 802.1X Authentication and Secure Channel Authentication Attributes

If the 802.1X authentication function or secure channel authentication function is not enabled under the port, relevant attributes configured cannot take effect.

#### Configuration Condition

None

#### Configure Port Authentication Method

802.1X authentication has two types, i.e. relay and termination.

The 802.1X authentication is composed of three parts, i.e. client, authentication device, and authentication server. According to the standard 802.1X protocol, the client interacts with the authentication server through EAP packets. The authentication device, as a "relay" in the interaction, encapsulates the EAP data sent by the client in other protocols, e.g. RADIUS protocol, and sends them to the authentication server. Likewise, the authentication device encapsulates the EAP data sent by the authentication server in an EAPOL packet and forwards them to the client. This way of interaction is called relay authentication. It requires the authentication server to support EAP protocol. The specific authentication mechanism supported by EAP relay authentication depends on the client and the authentication server.

The authentication server deployed earlier may not support EAP protocol. It needs to be configured with termination authentication. The EAP packets of the client will not be directly sent to the authentication

server. Instead, the authentication device will complete the EAP packet interaction with the client. After the authentication device obtains enough information about user authentication, the authentication information is sent to the authentication server for authentication.

EAP termination authentication supports PAP (Password Authentication Protocol) authentication and CHAP (Challenge Handshake Authentication Protocol) authentication.

Table 92 Configuring Port Authentication Mode

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Configure port authentication mode	<b>dot1x eap-relay { enable   disable }</b>	Mandatory By default, the port authentication mode is termination authentication.

---

 **Note**

Configure termination authentication. Currently, only the EAP authentication based on MD5 (Message Digest Algorithm Version 5) is supported. The 802.1X authentication and secure channel authentication functions support both relay and termination authentication.

When the client uses certificate authentication, the authentication port needs to be configured as relay authentication.

MAC address authentication supports termination authentication only.

## Configure Multicast Trigger

Some terminals have 802.1X authentication client, but the client cannot initiate authentication. The authentication process can only be triggered by the authentication device. The authentication device will periodically send a multicast packet requesting user name to the port configured with multicast trigger. After receiving this packet, the client responds to the authentication request of the authentication device and begins the authentication process.

Table 92 Configuring Multicast Trigger

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Enable multicast trigger	<b>dot1x multicast-trigger</b>	Mandatory  By default, the multicast trigger under the port is disabled.
Configure multicast trigger period	<b>dot1x multicast-period</b> <i>multicast-period-value</i>	Optional  By default, the multicast trigger time under the port is 15 seconds.



---

If the client doesn't support multicast trigger, its network card may display abnormally and cause failure of reauthentication.

---

### Configure Reauthentication Function

In order to detect whether the client is online, prevent abnormal client crashes from affecting the accuracy of charging, and prevent the client from being illegally used by others, the authentication device will periodically initiate a reauthentication request to the client. During this process, users are not required to input user name and password again.

Table 92 Configuring Reauthentication Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Configure Reauthentication Function	<b>dot1x reauthentication</b>	Mandatory  By default, the reauthentication function is enabled under the port.

### Configure the Maximum Number of Authentication Failures

When the number of authentication failures on the client reaches the upper limit, the client becomes quiet, during which period, the authentication device gives no response to the authentication request initiated by this client.

Table 92 Configuring Maximum Number of Authentication Failures

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Configure the upper limit of the maximum number of port authentication failures	<b>dot1x max-authfail</b> <i>max-authfail-value</i>	Mandatory  By default, the maximum number of authentication failures under the port is 1.

### Configure Function of Transparent Transmission of Packets

In the actual application environment, there may be intermediate devices between the terminal to be authenticated and the authentication device. If these intermediate devices cannot transparently transmit EAPOL packets, a normal authentication process is impossible. In order to enable a normal authentication process, you are required to enable the transparent transmission of EAPOL packet on the port of the intermediate device which receives EAPOL packet, and configure an uplink port for this port. If the port where the function of EAPOL packet transparent transmission is enabled receives an EAPOL packet, it will send it out from the configured uplink port. If the device directly connected to the uplink port is an authentication device, the authentication device will process the EAPOL packet after receiving it.

Table 1 Configuring Function of Packet Transparent Transmission

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Configure Function of Transparent Transmission of Packets	<b>dot1x eapol-relay</b> { <b>enable</b>   <b>disable</b> }	Mandatory  By default, the function of packet transparent transmission under the port is disabled.
Configure uplink port for packet transparent transmission	<b>dot1x eapol-relay uplink</b> { <b>interface</b> <i>interface-name</i>   <b>link-aggregation</b> <i>link-aggregation-id</i> }	Mandatory  By default, uplink port is not configured under the port.

### Configure Keepalive Function

In order to check whether the client is online, the authentication device will periodically send EAP-Request/Identity packet to the client. After receiving the EAP-Response/Identity packet from the client, it will send EAP-Request/MD5 Challenge packet to the client. If the authentication system receives the EAP-Response/MD5 Challenge packet, it confirms that the client is online normally, and sends an EAP-Success packet to notify the client of the successful keepalive.

Table 92 Configuring Keepalive Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Configure Keepalive Function	<b>dot1x keepalive { enable   disable }</b>	Mandatory  By default, the keepalive function under the port is disabled.
Configure keepalive time	<b>dot1x keepalive period</b> <i>period-value</i>	Optional  By default, the keepalive period under the port is 60 seconds.
Configure the times of keepalive packets retransmission	<b>dot1x keepalive retries</b> <i>retries-value</i>	Optional  By default, the maximum keepalive times is 3.
Configure keepalive type	<b>dot1x keepalive type</b> <b>{ request-identity   request-md5 }</b>	Optional  By default, the keepalive type under the port is standard keepalive.

## Note

The keepalive function needs the support of 802.1X authentication client software (the TC client of our company). If the client doesn't support this function, the keepalive will fail and the user will go offline.

## Configure Function of Not Waiting for Response of Server

Under relay authentication, the client may send some packets to which the server will not respond. These packets will make the session channels of authentication device and authentication server occupied so that subsequent client authentication fails. To avoid this, you can enable the function of not waiting for response of server under the port.

Table 92 Configuring Function of not Waiting for Response of Server

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected. After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Configure Function of Not Waiting for Response of Server	<b>dot1x nowait-result</b>	Mandatory By default, the function of not waiting for response of server under the port is disabled.

### 92.2.4 Configure MAC Address Authentication

Permit to configure both 802.1X authentication and MAC address authentication under the same port.

- When MAC address authentication is first conducted for terminal users, if the authentication succeeds, the 802.1X authentication initiated by these terminal users will not be processed. Otherwise, the 802.1X authentication initiated by these terminal users will be processed.
- If 802.1X authentication is first conducted for the terminal users, no MAC address

authentication is required.

### Configuration Condition

None

### Enable MAC Address Authentication Function

MAC address authentication is also called client-free authentication. This authentication method applies to both the terminals where client software cannot be installed for authentication, and the terminal users who do not have client software and can authenticate without inputting user name and password.

When configuring the parameters related to MAC address authentication under the port of authentication device, if the MAC address authentication function is not enabled on the port, relevant functions configured cannot take effect.

Table 92 Enabling MAC Address Authentication Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Enable MAC Address Authentication Function	<b>dot1x mac-authentication</b> { <b>enable</b>   <b>disable</b> }	Mandatory  By default, the MAC address authentication function under the port is disabled.



The MAC address authentication and port security functions can be both enabled under the same port, but port security IP rules and MAX rules are not allowed to configure.

The MAC address authentication and secure channel authentication functions cannot be both enabled under the same port.

### Configure MAC Address Authentication User Name Format

There are two types of user name and password formats for MAC address authentication: fixed and MAC address.

Fixed user name and password: When the authentication device receives the data packet of the terminal user, it will send the user name and password configured to the authentication server for authentication.

MAC address user name and password: The authentication will use the MAC address of the terminal user as user name and password. The MAC address format may either contain hyphen (e.g. 00-01-7a-00-00-01) or not contain hyphen (e.g. 00017a000001).

Table 2 Configuring Format of User Name for MAC Address Authentication

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Configure MAC Address Authentication User Name Format	<b>dot1x mac-authentication user-name-format { fixed account <i>account-value</i> password <i>password-value</i>  </b>	Mandatory  By default, the MAC address with hyphen is used as user name and

Step	Command	Description
	<b>mac-address [ with-hyphen   without-hyphen ] }</b>	password for MAC address authentication.

### Configure the Domain Name Used in Global MAC Authentication

This function can be enabled when the MAC authentication users connected to all ports on the device are required to be assigned to a specified domain for authentication.

By default, the domain name used in MAC authentication is not specified in the global mode. The domain used for user authentication should be the mandatory authentication domain configured on the port. If no such domain is configured on the port, use the domain contained in the user name. If the user name does not contain any domain, use the default domain of the aaa module.

After configuring on the port, the priority of the domain used by users who access mac authentication under the port is as follows: mandatory authentication domain configured on the port > domain contained in the fixed user name configured on the port > domain globally specified to be used for mac authentication > default domain of aaa module; the priority of the domain used by the 1x authentication users accessed under the port is as follows: mandatory authentication domain configured on the port > domain contained in the user name > default domain of the aaa module.

Table 92-16 Configuring Domain Name Used in Global MAC Authentication

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the domain name used in global MAC authentication	<b>dot1x mac-authentication domain <i>domain-name</i></b>	Mandatory By default, the domain name used in global MAC authentication is not configured under the port.

### Configure Domain Name Separator

The authentication device can manage users based on domains. If the authentication user name contains a domain name, the device uses the server in the corresponding AAA server group to authenticate, authorize and charge the user. If the authentication user name does not contain any domain name, it will use the default authentication server in the system for authentication. Therefore, the authentication device should be able to accurately resolve the user name and domain name in the user name. This is very critical in providing authentication services for users. Different clients support different user name and domain name

separators. In order to better manage and control the user access with different user name formats, it is required to specify the supported domain name separators on the authentication device.

At present, the domain name separators supported include @, \, and /.

When the domain name separator is '@', the format of authentication user name is username@domain.

When the domain name separator is '/', the format of authentication user name is username/domain.

When the domain name separator is '\', the format of authentication user name is domain\username.

In particular, username means a pure user name, and domain denotes a domain name. If the user name contains multiple domain name separators, the authentication device will identify the first one as the actual domain name separator, and all others will be considered as part of the domain name.

Table 3 Configuring Domain Name Separator

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Configure domain name separator	<b>dot1x domain-delimiter</b> <i>domain-delimiter-type</i>	Mandatory By default, the domain name separator under the port is '@'.



---

When using the user name with a domain name for authentication, corresponding authentication server group needs to be configured on the authentication device.

---

### Configure the Format of Authentication User Name

The authentication user is named in the format of 'username@domain', and the content following the separator '@' is a domain name. The authentication device determines which authentication server group is used to authenticate the user by resolving the domain name. Some earlier servers cannot accept user names that contain domain names. In this case, the authentication device needs to remove the domain names from the user names and only send the authentication user names to the server. Whether the authentication user name sent to the authentication device contains a domain name can be selected by configuring the format of authentication user name.

At present, the domain name separators supported include @, \, and /.

Table 92-18 Configuring Format of Authentication User Name

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Configure the format of authentication user name	<b>dot1x user-name-format</b> { with-domain   without-domain }	Mandatory  By default, the authentication user name with domain name is sent to the authentication server.

---

 **Note**

Configure the port that sends the authentication user name without domain name to the authentication server. Certificate authentication is not supported.

---

### Configure Authentication Packet Interaction Mode

In actual application scenarios, after most clients initiate authentication, the unicast/multicast authentication interaction mode is supported between the authentication device and the client. However, some authentication clients only recognize multicast authentication packets, i.e. those with a destination MAC address of 0180.C200.0003. In this case, the multicast authentication interaction mode can be configured under the port.

For most authentication clients, after the authentication device receives the EAP packet from the server for the first time, subsequent interactions with the client and the authentication server are all subject to the identifier contained in the server packet. Very few authentication clients are subject to the identifier generated by the authentication device during authentication. In this case, it is required to configure the function of caring about the identifier in EAP authentication packet under the port.

Table 92-19 Configuring Authentication Packet Interaction Mode

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Configure authentication interaction mode	<b>dot1x auth-mac { multicast   unicast }</b>	Mandatory By default, the unicast authentication packet

Step	Command	Description
		interaction mode is used under the port.
Function of caring about the identifier in EAP authentication packet	<b>dot1x identifier { match   ignore }</b>	Optional By default, the identifier in EAP authentication packet is not cared about.

---

### Note

Very few clients need to care about the identifier in EAP authentication interaction packet. Unless explicitly required, do not configure this function as far as possible.

---

## 92.2.5 Configure Common Attributes

When configuring the parameters of common attributes, if the 802.1X authentication function, secure channel authentication function or MAC address authentication function is not enabled on the port, relevant functions configured cannot take effect.

### Configuration Condition

When configuring the IP authorization function under the port, you are also required to configure the ARP keepalive function.

### Configure Control Direction

Port control direction has two types, i.e. two-way control and one-way control.

- Two-way control means the port cannot receive or forward packets.
- One-way control means the port cannot receive the packets from the client, though it can forward packets to the client.

It is used with the WOL (Wake On Lan) function. For some terminals, although they are dormant, their network card can process some special packets, such as WOL packets. After receiving the WOL packet, the network card will start the terminal device and begin working.

When the authentication function is enabled on the access port of the dormant terminal, you can configure the port as one-way control to ensure that WOL packets can be forwarded to the terminal normally. After the terminal is started, authentication activity can be initiated. It can normally access network resources after passing the authentication.

When sending WOL packets across network segments, it is required to configure ARP forwarding entries on the authentication device.

Table 92-20 Configuring Control Direction

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Configure Control Direction	<b>dot1x control-direction</b> { <b>both</b>   <b>in</b> }	Mandatory  By default, the port is controlled in both directions.

### Configure Authenticable Host List

After the function of authenticable host list is enabled, only the user whose MAC address is in the authenticable host list is permitted to conduct authentication activity. The authentications initiated by other users will be denied.

Table 92-21 Configure Authenticable Host List

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Configure Authenticable Host List	<b>dot1x auth-address</b> { <b>enable</b>   <b>disable</b>   <i>mac-address</i> }	Mandatory  By default, the authenticable host list under the port is disabled.

### Configure IP Authorization Function

Enable the IP authorization function under the port. If any change of the IP address of the authentication user is detected, the user will become offline. There are several modes:

**disable:** Disable mode. Under this mode, the IP address of user is not detected.

**dhcp-server:** DHCP Server mode. When configuring this mode, you are required to configure the DHCP Snooping function on the device. After the authentication user obtains IP address from the DHCP server, the device will record the binding relationship between authentication user and IP address. If any change of the IP address of the authentication user is detected, the user will become offline.

**radius-server:** RADIUS Server mode. RADIUS Server encapsulates in the RADIUS packet the IP address that the authentication user should use in the Frame-IP-Address field. The authentication device records the binding relationship between the user and this IP address. If it finds that the IP address of the user has changed, the user will become offline.

**Supplicant:** client mode. After the user passes the authentication for the first time, the binding relationship between the authentication user and the IP address is recorded on the device. If any change of the IP address of the user is detected, the user will become offline.

bind-mac-ip: MAC+IP binding mode. After the user passes the authentication for the first time, MAC+IP binding entries will be generated and saved. Then, only the IP address in the binding entries generated by the first authentication is permitted to access the network.

Table 92-22 Configuring IP Authorization Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Configure IP Authorization Function	<b>dot1x authorization ip-auth-mode { disable   dhcp-server   radius-server   supplicant   bind-mac-ip }</b>	Mandatory By default, the IP authorization function under the port is disabled.

### Configure the Maximum Times of Transmitting Authentication Request Packets

After receiving the EAPOL-Start packet sent by the client, the authentication device will send an authentication request EAP-Request/Identity packet to the client. If the authentication device fails to receive the response packet, the packet will be retransmitted. This function is used to configure the maximum times of sending EAP-Request/Identity packets. If the times of sending exceed the configured upper limit, the authentication device will consider the client has disconnected and end the authentication activity.

For the process of retransmitting EAP-Request/Identity packet, see the figure below:

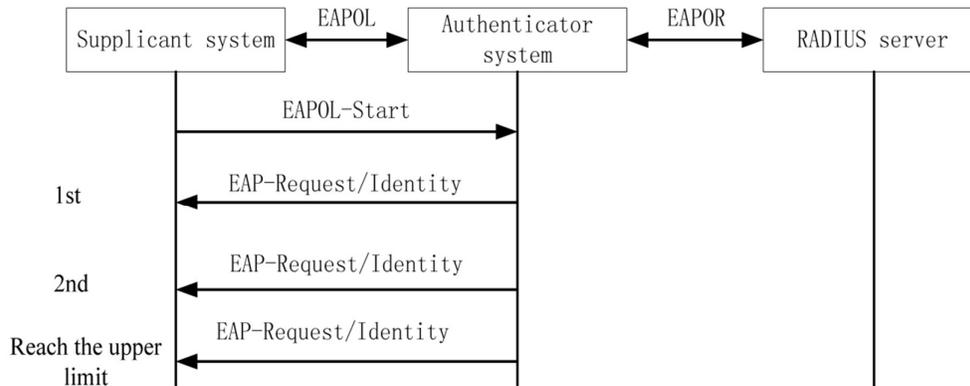


Figure 12-4 Retransmission of EAP-Request/Identity Packet

Table 92-23 Configuring the Maximum Times of Transmitting Authentication Request Packets

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Configure the Maximum Times of Transmitting Authentication Request Packets	<b>dot1x max-reauth</b> <i>count</i>	Mandatory  By default, the maximum times of transmitting authentication request packets under the port are 3.

### Configure the Maximum Times of Transmitting Authentication Packets

During the process of authentication, the authentication device sends other EAP-Request packets than EAP-Request/Identity packet to the client, such as EAP-Request/MD5 challenge packet. If the authentication device fails to receive the response packet, the packet will be retransmitted. This function is used to configure the maximum times of sending these packets. If the times of sending exceed the configured upper limit, the authentication device will consider the client authentication fails.

For the process of retransmitting EAP-Request packet, see the figure below:

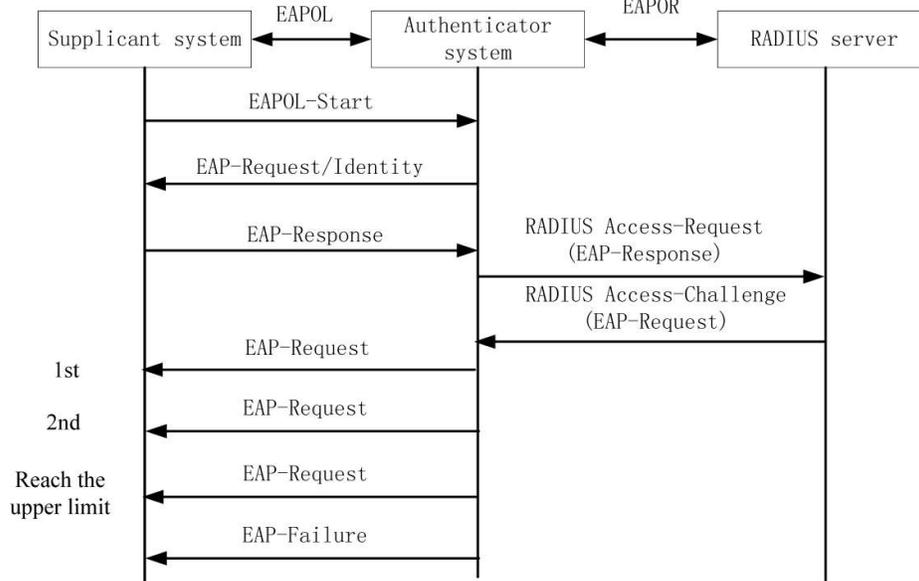


Figure 1 Retransmission of EAP-Request Packet

Table 92-24 Configuring the Maximum Times of Transmitting Authentication Packets

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter

Step	Command	Description
		the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Configure the Maximum Times of Transmitting Authentication Packets	<b>dot1x max-req count</b>	Mandatory By default, the maximum times of transmitting authentication packets under the port are 2.

### Configure Function of Data Logging

After the data logging function is enabled, the authentication device will record the information about the user's going online and offline and the change of user information for the convenience of troubleshooting.

Table 92-25 Configuring Data Logging Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected. After you enter the layer-2 Ethernet interface
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.

Step	Command	Description
Configure Function of Data Logging	<b>dot1x logging security-data {abnormal-logout   failed-login   normal-logout   successful-login   information}*</b>	Mandatory  By default, the data logging function is not enabled under the port.

### Configure ARP Keepalive Function

After the terminal user authentication succeeds, to check whether the user is online, the authentication device can send ARP request packet to the authenticated user. It identifies whether the user is online through the ARP response packet it can receive or not from the user.

Table 92-26 Configuring ARP Keepalive Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Configure ARP Keepalive Function	<b>dot1x client-probe</b> { <b>enable</b>   <b>disable</b> }	Mandatory  By default, the ARP keepalive function under the port is disabled.

---

 **Note**

To normally trigger the ARP keep-alive function, the authentication device has to obtain the IP address of the authenticated user. If the ARP response packet fails to be received from the authentication device during the protection period, the user will become offline.

---

### Configure the Maximum Number of Users on Port

After the number of users authenticated under the port reaches the upper limit configured, the authentication system no longer responds to the authentication request initiated by the new user.

Table 92-27 Configuring Maximum Number of Users on Port

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Configure the Maximum Number of Users on Port	<b>authentication max-user-num</b> <i>max-uer-num-value</i>	Mandatory  By default, at most 256 users are permitted to access under the port.

---

 **Note**

---

Under the port, configure as Macbased access control. Otherwise, the configured number of users permitted to access cannot take effect.

---

### Configure IP ACL Prefix Name

After the terminal user authentication succeeds, when the number of the IP ACL issued by the server is greater than 2000, the IP ACL named "IP ACL prefix name" + "ACL number" needs to be configured in the device. For example, if the server issues ACL 2001, the IP ACL named "assignacl-2001" should be configured on the device.

Table 92-28 Configuring IP ACL Prefix Name

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure IP ACL Prefix Name	<b>dot1x number-acl-prefix</b> <i>number-acl-prefix-name</i>	Mandatory By default, the IP ACL prefix name is "assignacl-".

---

### Note

When the access control method is configured as portbased host-mode multi-hosts, the function of issuing ACL is not valid.

---

### Configure Default Valid VLAN

When the server issues no VLAN (Auto VLAN), to make the users who pass authentication communicate within the specified VLAN, you can use this configuration to specify a VLAN.

Table 92-29 Configuring Default Valid VLAN

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure Default Valid VLAN	<b>dot1x default-active-vlan</b> <i>default-active-vlan-id</i>	Mandatory

Step	Command	Description
		By default, no default valid VLAN is configured under the port.

### Note

After the user authentication succeeds, the priority of binding with VLAN is as follows: VLAN issued by the server, default valid VLAN, and VLAN to which the port PVID belongs.

When Macbased access control is configured under the port, the default valid VLAN will take effect only when the port meets the following conditions: VLAN mode is hybrid and MAC VLAN is enabled.

### Configure Function of Permitting Unauthenticated Users to Communicate in the VLAN of PVID

When multiple terminals access the port, each of them should have access control. This command can be enabled for the network resources which some terminals intend to access even if they cannot initiate 802.1X authentication. After this function is enabled, the unauthenticated terminal user can normally communicate in the VLAN of PVID.

This function can be normally used only when it meets the following conditions:

- 802.1X authentication or MAC address authentication is enabled on the port.
- The port access control is Macbased.
- The port VLAN mode is Hybrid.
- The function of receiving Untag packets only is enabled under the port.

Table 92-30 Configuring Function of Permitting Unauthenticated Users to Communicate in the VLAN of PVID

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure Function of Permitting Unauthenticated Users to Communicate in the VLAN of PVID	<b>dot1x native-vlan-free</b>	Mandatory By default, the function of permitting unauthenticated users to communicate in

Step	Command	Description
		the VLAN of PVID is disabled under the port.

## Note

After this function is enabled on the port, the function of receiving Untag packets only should also be enabled (configure the following command under the port: `switchport accept frame-type untag`) to guarantee the packets sent by the users who fail to pass the authentication are forwarded within the VLAN of PVID only.

It is recommended that this function be used with the VLAN issued by the server or the default valid VLAN configured.

This function does not support secure channel authentication.

### Configure Port Access Control Method

There are two types of port access control: Portbased and Macbased.

Portbased access control: Only one user is permitted to pass authentication under the port.

Macbased access control: Multiple users are permitted to pass authentication under the port. They cannot access the network without passing authentication.

The Portbased access control also has two modes: Multi-hosts and Single-host.

Multi-hosts: After one user passes authentication, other users under the port can access the network without authentication.

Single-host: Under the port, only one user is permitted to pass authentication and access the network. Other users cannot access the network or pass authentication.

Table 92-31 Configuring Port Access Control Method

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.

Step	Command	Description
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Configure access control method	<b>authentication port-method { macbased   portbased }</b>	Mandatory  By default, user authentication method is enabled under the port.
Portbased access control method	<b>authentication port-method portbased host-mode { multi-hosts   single-host }</b>	Optional  By default, Multi-hosts authentication is enabled under the port.

### Note

When configuring the host mode under portbased access control, you should guarantee that the access control method has been configured as Portbased.

## Configure Guest VLAN

The user can obtain 802.1X client software from the Guest VLAN to upgrade the client, or execute other application (e.g. anti-virus software and OS patches) upgrading.

Table 92-32 Configuring Guest VLAN

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Configure Guest VLAN	<b>authentication guest-vlan</b> <i>guest-vlan-id</i>	Mandatory  By default, no Guest VLAN is configured under the port, and the value range is 1~4094.

---

### Note

The Guest VLAN of the port cannot be applied to the dynamic VLAN. If the VLAN ID specified by the Guest VLAN is automatically created by GVRP, then the Guest VLAN can be successfully configured, but it will not take effect.

To ensure various functions can be normally used, please assign different VLAN IDs to Voice VLAN, Private VLAN and Guest VLAN.

---

### Configure Guest ACL

If the user fails to pass authentication, you can restrict it from accessing resources in the Guest VLAN by configuring Guest ACL under the port.

Table 92-33 Configuring Guest ACL

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected. After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Configure Guest ACL	<b>authentication guest-acl</b> <i>guest-acl-name</i>	Mandatory By default, Guest ACL rules are not configured under the port.

---

### Note

If no Guest VLAN is configured under the port, the configuration of Guest ACL will not take effect.

Guest ACL only takes effect under the Macbased port access control method.

Corresponding ACL rules have been configured in the authentication device.

---

### Configure Critical VLAN

When the user uses RADIUS authentication, if the authentication fails due to the unreachable authentication server, this user can access resources in the specified VLAN. This VLAN is called a Critical VLAN.

When the port is configured with portbased access control method, and there is user authentication on the port, yet all authentication servers are unreachable, the port will be added to the Critical VLAN, and all users under the port can access resources in the Critical VLAN.

When the port is configured with Macbased access control method, and there is user authentication on the port, yet all authentication servers are unreachable, the user can only access resources in the Critical VLAN.

When the port is configured with Macbased access control method, it can be normally used only when it meets the following conditions:

- The port VLAN mode is Hybrid.
- Enable the MAC VLAN function on the port. When the user in the Critical VLAN initiates an authentication activity, if the authentication server is still unreachable, the user maintains in the Critical VLAN. If the authentication server is reachable, the user exits the Critical VLAN with the authentication result.

After the port is added to the critical VLAN and the authentication device is configured with the AAA detection function, when the authentication server is found reachable, if the critical-vlan recovery reinitialize function is configured, then:

- If the port is configured with Macbased access control method, the port added to the Critical VLAN will actively send unicast packets to all users in the Critical VLAN, triggering user reauthentication.
- If the port is configured with Portbased access control method, the port added to the Critical VLAN will actively send multicast packets to trigger user reauthentication.

Table 4 Configuring Critical VLAN

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Configure Critical VLAN	<b>authentication critical-vlan</b> <i>critical-vlan-id</i>	Mandatory  By default, no Critical VLAN is configured under the

Step	Command	Description
		port, and the value range is 1~4094.
Configure port recovery and trigger authentication	<b>authentication critical-vlan recovery-action reinitialize</b>	Optional By default, after the authentication server is found reachable, the port leaves the Critical VLAN only.

---

## Note

- This function supports RADIUS authentication only.
  - If the device is configured with radius and escape functions, i.e., aaa authentication dot1x radius none and critical vlan, when the user is authenticated and the authentication server is unreachable, the user will not enter the critical VLAN but escape directly; if only the escape function, i.e. aaa authentication dot1x none, and critical vlan are configured, when the user is authenticated, the escape function takes effect.
  - When only Guest VLAN is configured under the port, the users who fail to pass the authentication are within the Guest VLAN. When both Guest VLAN and Critical VLAN functions are configured under the port, the user will enter the Critical VLAN if the authentication fails due to the unreachable authentication server, or the Guest VLAN if the authentication fails due to other reasons.
  - For details of the AAA detection function, see the AAA configuration-related section.
- 

### Configure User Authentication Migration Function

The user authentication migration function applies to the scenarios where the same user (depending on the terminal MAC address) migrates from one authentication port to another in the same device. When the user authentication migration function is disabled, after a user is authenticated on one port of the device, it is not permitted to initiate authentication on another authentication port of the device; when the user authentication migration function is enabled, after the user is authenticated on one port, and the device finds that the user has migrated to another authentication port, the device deletes the authentication information on the original port and then permits the user to initiate authentication on a new authentication port.

No matter whether the user authentication migration function is enabled, the device will record a log once it finds user migration between authentication ports.

Table 5 Configuring User Authentication Migration Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected. After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Configure User Authentication Migration Function	<b>authentication station-move { enable   disable }</b>	Mandatory By default, the user authentication migration function is disabled.

### Configure Timer Parameters

The timer parameters under the port include re-authperiod, quiet-period, server-timeout, supp-timeout, and MAC address authentication user offline-detect.

**Re-authperiod:** After the reauthentication function is configured under the port, the authentication device periodically initiates reauthentication requests to the client, which applies to 802.1X authentication.

**Quiet-period:** When the client reaches the maximum number of authentication failures, the authentication device will respond to the authentication request from the client again after the quiet period expires. This applies to 802.1X authentication and MAC address authentication.

**Server-timeout:** If the authentication device fails to receive the server response packet within the specified time, it is considered that it has disconnected with the server. This applies to 802.1X authentication and MAC address authentication.

**Supp-timeout:** If the authentication device fails to receive response packet from the 802.1X client within the specified time, it is considered that it has disconnected with the user. This applies to 802.1X authentication.

MAC address authentication user offline-detect: After MAC address authentication is enabled, the port periodically checks whether the user is online. This applies to MAC address authentication.

Table 92-36 Configuring Timer Parameters

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Configure Timer Parameters	<b>dot1x timeout { re-authperiod</b> <i>re-authperiod-value</i> <b>  quiet-period</b> <i>quiet-period-value</i> <b>  server-timeout</b> <i>server-timeout-value</i> <b>  supp-timeout</b> <i>supp-timeout-value</i> <b>  offline-detect</b> <i>offline-detect-value</i> <b>}</b>	Mandatory  By default,  the reauthentication time under the port is 3600 seconds, and the value range is 5~65535;  the quiet period is 60 seconds, and the value range is 1~65535;  the timeout time of the server is 30 seconds, and the value range is 5~3600;  the timeout time of the client is 30 seconds, and the value range is 5~3600;  the client offline detection time is 300 seconds, and the value range is 5~3600.

**Configure MAB function**

After the terminal passes the MAC address authentication, when it's necessary to use higher access rights through client authentication, you can enable this function.

Table 92-37 Enabling MAB Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Enable 802.1X Authentication	<b>dot1x port-control { enable   disable }</b>	Mandatory  By default, the 802.1X authentication function under the port is disabled.
Enable MAC Address Authentication Function	<b>dot1x mac-authentication { enable   disable }</b>	Mandatory  By default, the MAC address authentication function under the port is disabled.
Enable MAB function	<b>dot1x after-mac-auth { enable   disable }</b>	Mandatory  By default, the MAB function under the port is disabled.

### Restore Default Configurations of Port

Recover the default configuration of 802.1X authentication and MAC address authentication under the port.

Table 92-38 Recovering Default Configuration of Port

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Restore Default Configurations of Port	<b>dot1x default</b>	Mandatory  The 802.1X authentication and MAC address authentication functions under the port are disabled, related configuration parameters are recovered to default values, and the default configuration parameters do not take effect.

---

 **Note**

The command `show dot1x` is used to view detailed default authentication configuration parameters.

---

**Configure mandatory authentication domain for port**

This function can be enabled when the users to be authenticated on the port are required to be assigned to a specified domain for authentication.

By default, no mandatory authentication domain is configured for the port. The domain used for user authentication should be that carried by the user. If there is no domain in the user name, use the default domain of the aaa module.

After configuration on the port, the user can use the domains by the following priority: domain configured under the port > domain carried by the user > default domain of aaa module.

Table 92-39 Enabling Mandatory Authentication Domain Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Enable 802.1X mandatory authentication domain function	<b>dot1x authentication domain</b> <i>domain-name</i>	Mandatory  By default, no mandatory authentication domain is configured under the port.

## 92.2.6 802.1X monitoring and maintaining

Table 92-40 802.1X Monitoring and Maintaining

Command	Description
<b>clear dot1x statistic</b> [ <b>interface</b> <i>interface-name</i>   <b>interface link-aggregation</b> <i>link-aggregation-id</i>   <b>mac</b> { <i>mac-address</i>   <b>all</b> } ]	Clear authentication statistics
<b>clear dot1x auth-fail-user history</b> [ <b>mac</b> <i>mac-address</i> ]	Clear record of failed authentication
<b>show authentication user</b> [ <b>interface</b> <i>interface-name</i>   <b>interface link-aggregation</b> <i>link-aggregation-id</i>   <b>mac</b> <i>mac-address</i>   <b>summary</b> ]	Show the information of authentication management users
<b>show authentication intf-status</b> [ <b>interface</b> <i>interface-name</i>   <b>interface link-aggregation</b> <i>link-aggregation-id</i> ]	Show the information of authentication status
<b>show dot1x</b>	Show default configurations of authentication
<b>show dot1x auth-fail-user history</b> [ <b>recent</b>   <b>mac</b> <i>mac-address</i> ]	Show the information of authentication failure
<b>show dot1x auth-address</b> [ <i>mac-address</i>   <b>interface</b> <i>interface-name</i>   <b>interface link-aggregation</b> <i>link-aggregation-id</i> ]	Show the information of authenticable host list
<b>show dot1x config</b> [ <b>interface</b> <i>interface-name</i>   <b>interface link-aggregation</b> <i>link-aggregation-id</i> ]	Show configurations of authentication
<b>show dot1x free-ip</b>	Show configuration information of secure channel.
<b>show dot1x global config</b>	Show the information of global configuration
<b>show dot1x statistic</b> [ <b>interface</b> <i>interface-name</i>   <b>interface link-aggregation</b> <i>link-aggregation-id</i>   <b>mac</b> { <i>mac-address</i>   <b>all</b> } ]	Show authentication statistics
<b>show dot1x user</b> [ <b>interface</b> <i>interface-name</i>   <b>interface link-aggregation</b> <i>link-aggregation-id</i>   <b>summary</b> ]	Show user information

## 92.3 Typical Configuration Example of 802.1X Function

### 92.3.1 Configure Portbased Authentication of 802.1X

#### Network Requirements

- PC1 and PC2 on the same LAN access the IP network through the Device where 802.1X access control is enabled;
- RADIUS authentication is used as an authentication method;
- Users can access the Update Server only when they fail to pass authentication. They are permitted to access the IP Network once it passes the authentication;
- After one user on the LAN passes authentication, other users on this LAN can access the IP Network without authentication.

#### Network Topology

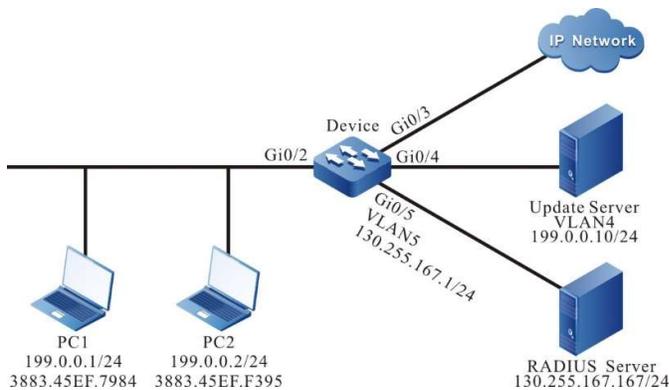


Figure 2 Network Topology for Configuring Portbased Authentication of 802.1X

#### Configuration Steps

Step 1: Configure VLAN and port link type on Device.

#Create VLAN2~VLAN5 on the Device.

```
Device#configure terminal
Device(config)# vlan 2-5
Device(config)#exit
#Configure the link type of port gigabitethernet0/2 to Access to allow services of VLAN 2 to pass.
```

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode access
Device(config-if-gigabitethernet0/2)#switchport access vlan 2
Device(config-if-gigabitethernet0/2)#exit
```

#Configure the link type of the ports gigabitethernet 0/3~gigabitethernet 0/5 on the Device as Access, allowing the services of VLAN3~VLAN5 to pass. (Omitted)

Step 2: Configure interface IP address for the Device.

#Configure the IP address of VLAN5 as 130.255.167.1/24.

```
Device(config)#interface vlan 5
Device(config-if-vlan5)#ip address 130.255.167.1 255.255.255.0
Device(config-if-vlan5)#exit
```

Step 3: Configure AAA authentication.

#Enable AAA on the Device and use RADIUS authentication. The server key is admin, priority 1, and RADIUS server address 130.255.167.167/24.

```
Device(config)#domain system
Device(config-isp-system)# aaa authentication dot1x radius-group radius
Device(config-isp-system)#exit
Device(config)#aaa server group radius radius
Device(config-sg-radius-radius)#server 130.255.167.167 priority 1 key admin
```

Step 4: Configure AAA server.

#On AAA server, configure user name, password and key value as admin. (Omitted)

#On the AAA server, configure three attributes for the Auto VLAN issued by RADIUS: 64 as VLAN, 65 as 802, and 81 as VLAN3. (Omitted)

Step 5: Configure 802.1X authentication for the port.

#Enable 802.1X authentication on the port and configure Portbased mode.

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#dot1x port-control enable
Device(config-if-gigabitethernet0/2)#authentication port-method portbased
Device(config-if-gigabitethernet0/2)#exit
```

#Configure the Guest VLAN of the port as VLAN4.

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#authentication guest-vlan 4
Device(config-if-gigabitethernet0/2)#exit
```

Step 6: Check the result.

#Before passing authentication, gigabitethernet0/2 is added to the Guest VLAN. At this moment, both PC1 and PC2 users are within VLAN4 and permitted to access the Update Server.

```
Device#show vlan 4
```

NO.	VID	VLAN-Name	Owner	Mode	Interface
1	4	VLAN0004	static	Untagged	gi0/2 gi0/4

#Verify that PC1 can pass the authentication, and the authentication server issues VLAN3. At this moment, both PC1 and PC2 users are within VLAN3 and can access the IP Network.

Device#show dot1x user

```
-----
NO 1 : MAC_ADDRESS= 3883.45ef.7984 STATUS=   Authorized   USER_NAME=  admin
      VLAN=         3      INTERFACE=  gi0/2      USER_TYPE=  DOT1X
      AUTH_STATE=  AUTHENTICATED  BACK_STATE=  IDLE      IP_ADDRESS=  Unknown
      IPV6_ADDRESS= Unknown
```

Online time: 0 week 0 day 0 hours 0 minute 51 seconds

Total: 1 Authorized: 1 GetIP: 0 Unauthorized/guest/critical: 0/0/0 Unknown: 0

### 92.3.2 Configure Macbased Authentication of 802.1X

#### Network Requirements

- Both PC1 and PC2 access the IP network through the Device which uses 802.1X access control;
- RADIUS authentication is used as an authentication method;
- PC can access the Update Server only when it fails to pass authentication. It permitted to access the IP Network once it passes the authentication;
- After one user on the LAN passes authentication, other users on this LAN still need to pass the authentication prior to accessing the IP Network.

#### Network Topology

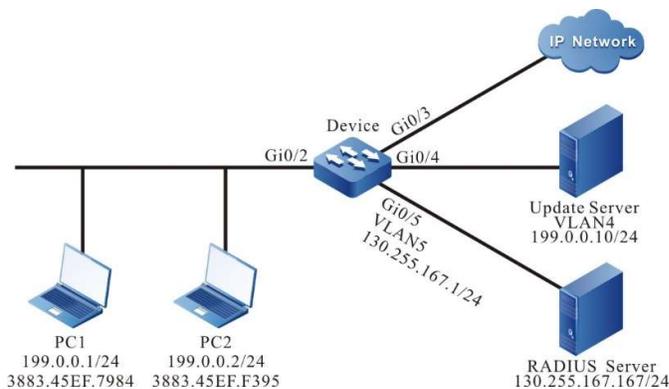


Figure 92 Network Topology for Configuring Macbased Authentication of 802.1X

#### Configuration Steps

Step 1: Configure VLAN and port link type on Device.

#Create VLAN2~VLAN5 on the Device.

```
Device#configure terminal
Device(config)#vlan 2-5
Device(config)#exit
```

#Configure the link type of port gigabitethernet 0/2 to Hybrid to allow services of VLAN2 to pass, and configure PVID to 2.

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport hybrid untagged vlan 2
Device(config-if-gigabitethernet0/2)#switchport hybrid pvid vlan 2

Device(config-if-gigabitethernet0/2)#exit
```

#Configure the link type of the ports gigabitethernet 0/3~gigabitethernet 0/5 on the Device as Access, allowing the services of VLAN3~VLAN5 to pass. (Omitted)

Step 2: Configure interface IP address for the Device.

#Configure the IP address of VLAN5 as 130.255.167.1/24.

```
Device(config)#interface vlan 5
Device(config-if-vlan5)#ip address 130.255.167.1 255.255.255.0
Device(config-if-vlan5)#exit
```

Step 3: Configure AAA authentication.

#Enable AAA authentication on the Device, authentication method RADIUS, server key admin, priority 1, and RADIUS server address 130.255.167.167/24.

```
Device(config)#domain system
Device(config-isp-system)# aaa authentication dot1x radius-group radius
Device(config-isp-system)#exit
Device(config)#aaa server group radius radius
Device(config-sg-radius-radius)#server 130.255.167.167 priority 1 key admin
```

Step 4: Configure AAA server.

#On AAA server, configure user name, password and key value as admin. (Omitted)

#On the AAA server, configure three attributes for the Auto VLAN issued by RADIUS: 64 as VLAN, 65 as 802, and 81 as VLAN3. (Omitted)

Step 5: Configure 802.1X authentication.

#Enable 802.1X authentication on the port and configure the authentication mode as Macbased.

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#dot1x port-control enable
Device(config-if-gigabitethernet0/2)#authentication port-method macbased
Device(config-if-gigabitethernet0/2)#exit
```

#Enable the MAC VLAN of gigabitethernet0/2.

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#mac-vlan enable
Device(config-if-gigabitethernet0/2)#exit
```

#Configure the Guest VLAN of the port as VLAN4.

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#authentication guest-vlan 4
Device(config-if-gigabitethernet0/2)#exit
```

Step 6: Check the result.

#Before passing authentication, gigabitethernet0/2 is added to the Guest VLAN. At this moment, both PC1 and PC2 users are within VLAN4 and can access the Update Server.

```
Device#show vlan 4
-----
NO. VID VLAN-Name          Owner Mode  Interface
-----
1  4  VLAN0004                static Untagged gi0/2 gi0/4
```

#After PC1 users initiate authentication and successfully pass the authentication, they are within Auto VLAN3 and can access the IP Network. At this moment, PC2 still needs to pass the authentication prior to accessing the IP Network.

```
Device#show dot1x user
-----
NO 1 : MAC_ADDRESS= 3883.45ef.7984 STATUS=   Authorized   USER_NAME=  admin
      VLAN=      3      INTERFACE=  gi0/2      USER_TYPE=  DOT1X
      AUTH_STATE= AUTHENTICATED BACK_STATE=  IDLE       IP_ADDRESS=  Unknown
      IPV6_ADDRESS= Unknown
```

Online time: 0 week 0 day 0 hours 0 minute 51 seconds

Total: 1 Authorized: 1 GetIP: 0 Unauthorized/guest/critical: 0/0/0 Unknown: 0

#After PC2 users input incorrect user name or password authentication fails, PC2 users are within Guest VLAN4 and can access the Update Server.

```
Device#show dot1x user
-----
NO 1 : MAC_ADDRESS= 3883.45ef.f395 STATUS=   Unauth(guest) USER_NAME=  admin
      VLAN=      4      INTERFACE=  gi0/2      USER_TYPE=  DOT1X
      AUTH_STATE= GUEST_HELD  BACK_STATE=  IDLE       IP_ADDRESS=  Unknown
      IPV6_ADDRESS= Unknown
```

Total:1 Authorized: 0 Unauthorized/guest/critical: 0/1/0 Unknown: 0

### 92.3.3 Configure Transparent Transmission Mode of 802.1X

#### Network Requirements

- PC connects to Device2 where 802.1X access control is enabled through Device1 to access the IP Network.
- Device1 enables the function of transparent transmission, and Device 2 uses RADIUS

authentication.

- PC can access the IP Network once it passes authentication.

## Network Topology

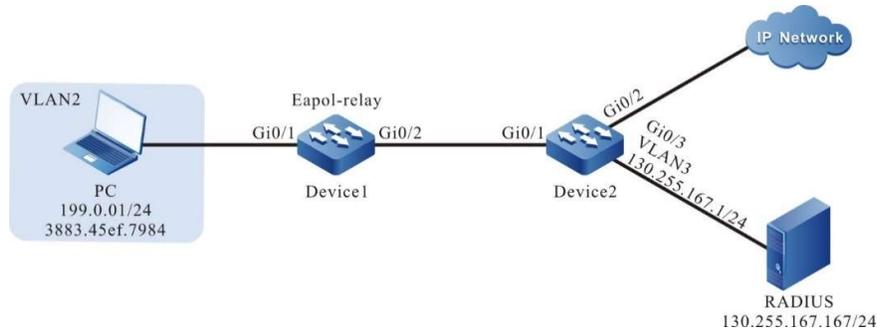


Figure 92 Network Topology for Configuring Transparent Transmission Mode of 802.1X

## Configuration Steps

Step 1: Configure VLAN and port link type on Device2.

#Create VLAN2-VLAN3 on Device2.

```
Device2#configure terminal
Device2(config)#vlan 2-3
Device2(config)#exit
```

#Configure the link type of port gigabitethernet 0/1 to Access to allow services of VLAN 2 to pass.

```
Device2(config)#interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#switchport mode access
Device2(config-if-gigabitethernet0/1)#switchport access vlan 2
Device2(config-if-gigabitethernet0/1)#exit
```

#Configure the link type of the ports gigabitethernet 0/2~ gigabitethernet 0/3 on Device2 as Access, allowing the services of VLAN2~VLAN3 to pass. (Omitted)

Step 2: Configure the interface IP address of Device2.

#Configure the IP address of VLAN3 as 130.255.167.1/24.

```
Device2(config)#interface vlan 3
Device2(config-if-vlan3)#ip address 130.255.167.1 255.255.255.0
Device2(config-if-vlan3)#exit
```

Step 3: Configure AAA authentication.

#Enable AAA authentication on Device2, authentication method RADIUS, server key admin, priority 1, and RADIUS server address 130.255.167.167/24.

```
Device(config)#domain system
Device(config-isp-system)# aaa authentication dot1x radius-group radius
Device(config-isp-system)#exit
```

```
Device(config)#aaa server group radius radius
Device(config-sg-radius-radius)#server 130.255.167.167 priority 1 key admin
```

Step 4: Configure AAA server.

#On AAA server, configure user name, password and key value as admin (omitted).

Step 5: Configure the port VLAN of Device1.

#Configure the link type of ports gigabitethernet0/1~gigabitethernet0/2 on Device1 as Access, allowing the services of VLAN2 to pass. (Omitted)

Step 6: On Device1, enable the function of 802.1X transparent transmission.

#Configure 802.1X transparent transmission mode on the port gigabitethernet0/1 of Device1, with the uplink port being gigabitethernet0/2.

```
Device1(config)#interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#dot1x eapol-relay enable
Device1(config-if-gigabitethernet0/1)#dot1x eapol-relay uplink interface gigabitethernet 0/2
Device1(config-if-gigabitethernet0/1)#exit
```

Step 7: Configure 802.1X authentication mode on Device2.

#Enable 802.1X authentication on gigabitethernet0/1 and configure the port authentication mode as Portbased.

```
Device2(config)#interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#dot1x port-control enable
Device2(config-if-gigabitethernet0/1)#authentication port-method portbased
Device2(config-if-gigabitethernet0/1)#exit
```

Step 8: Check the result.

#PC users can successfully pass the authentication and access the IP Network.

```
Device2#show dot1x user
```

```
-----
```

```
NO 1 : MAC_ADDRESS= 3883.45ef.7984 STATUS=   Authorized   USER_NAME=  admin
      VLAN=      2      INTERFACE=  g10/1      USER_TYPE=  DOT1X
      AUTH_STATE= AUTHENTICATED BACK_STATE=  IDLE      IP_ADDRESS=  Unknown
      IPV6_ADDRESS= Unknown
```

Online time: 0 week 0 day 0 hours 0 minute 51 seconds

Total: 1 Authorized: 1 GetIP: 0 Unauthorized/guest/critical: 0/0/0 Unknown: 0

### 92.3.4 Configure 802.1X Free-Client Authentication

#### Network Requirements

- The network printer accesses IP network through the Device which uses 802.1X access control.
- The Device periodically conducts offline detection over the network printer.
- Use RADIUS authentication.
- After passing authentication, the network printer can perform the printing tasks from IP network.

#### Network Topology

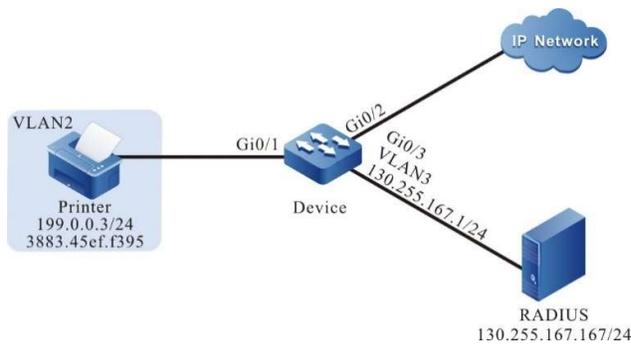


Figure 92 Network Topology for Configuring 802.1X Free-client Authentication

#### Configuration Steps

Step 1: Configure VLAN and port link type on Device.

#Create VLAN2-VLAN3 on the Device.

```
Device#configure terminal
Device(config)#vlan 2-3
Device(config)#exit
```

#Configure the link type of port as Access on gigabitethernet 0/1, permitting the services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode access
Device(config-if-gigabitethernet0/1)#switchport access vlan 2
Device(config-if-gigabitethernet0/1)#exit
```

#Configure the link type of port as Access on gigabitethernet 0/2~ gigabitethernet 0/3 of the Device, allowing the services of VLAN2~VLAN3 to pass. (Omitted)

Step 2: Configure interface IP address for the Device.

#Configure the IP address of VLAN3 as 130.255.167.1/24.

```
Device(config)#interface vlan 3
Device(config-if-vlan3)#ip address 130.255.167.1 255.255.255.0
Device(config-if-vlan3)#exit
```

Step 3: Configure AAA authentication.

#Enable AAA authentication on the Device, authentication method RADIUS, server key admin, priority 1, and RADIUS server address 130.255.167.167/24.

```
Device(config)#domain system
Device(config-isp-system)# aaa authentication dot1x radius-group radius
Device(config-isp-system)#exit
Device(config)#aaa server group radius radius
Device(config-sg-radius-radius)#server 130.255.167.167 priority 1 key admin
```

Step 4: Configure AAA server.

#On AAA server, configure user name, password and key value as admin. (Omitted)

Step 5: Configure 802.1X authentication.

#Configure 802.1X free-client authentication mode, and use the MAC address of the network printer as user name and password.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#dot1x mac-authentication enable
Device(config-if-gigabitethernet0/1)#exit
```

#Configure the Device to periodically conduct offline detection over the printer every 120 seconds.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#dot1x timeout offline-detect 120
Device(config-if-gigabitethernet0/1)#exit
```

Step 6: Check the result.

#The network printer can pass authentication and perform the printing tasks from IP network.

```
Device#show dot1x user
```

```
-----
NO 1 : MAC_ADDRESS= 3883.45ef.f395 STATUS= Authorized USER_NAME= 38-83-45-ef-f3-95
      VLAN= 2 INTERFACE= gi0/1 USER_TYPE= DOT1X
      AUTH_STATE= AUTHENTICATED BACK_STATE= IDLE IP_ADDRESS= 199.0.0.3
      IPV6_ADDRESS= Unknown
```

```
Online time: 0 week 0 day 0 hours 1 minutes 6 seconds
Total: 1 Authorized: 1 GetIP: 0 Unauthorized/guest/critical: 0/0/0 Unknown: 0
```

## 92.3.5 Configure Secure Channel

### Network Requirements

- PC1 and PC2 on the same LAN access the IP network through the Device where secure channel access control is enabled;
- RADIUS authentication is used as an authentication method;
- PC1 can access the Update Server prior to passing authentication. It is permitted to access the Update Server once it passes the authentication;
- PC2 can access the Update Server and IP Network without authentication.

### Network Topology

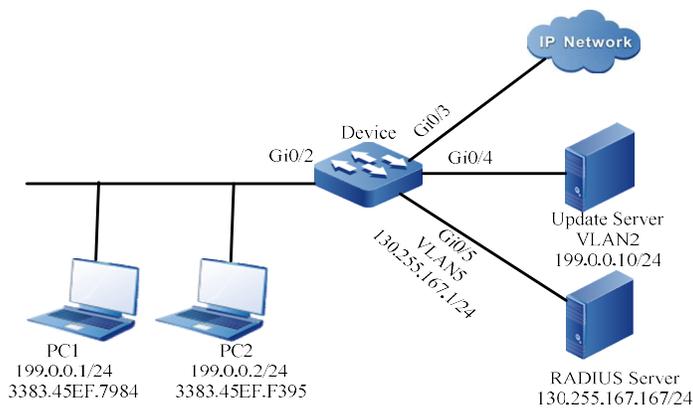


Figure 92 Network Topology for Configuring Secure Channel

### Configuration Steps

Step 1: Configure VLAN and link type on the port.

#Create VLAN2 and VLAN5 on the Device.

```
Device#configure terminal
Device(config)#vlan 2,5
Device(config)#exit
```

#Configure the link type of gigabitethernet0/2 to Access to allow services of VLAN 2 to pass.

```
Device#configure terminal
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)# switchport mode access
```

```
Device(config-if-gigabitethernet0/2)# switchport access vlan 2
Device(config-if-gigabitethernet0/2)#end
```

#Configure the link type of port as Access on gigabitethernet 0/3~gigabitethernet 0/4 of the Device to allow services of VLAN 2 to pass, and as Trunk on gigabitethernet 0/5 to allow services of VLAN5 to pass.

(Omitted)

Step 2: Configure interface IP address for the Device.

#Configure the IP address of VLAN5 as 130.255.167.1/24.

```
Device#configure terminal
Device(config)#interface vlan 5
Device(config-if-vlan5)#ip address 130.255.167.1 255.255.255.0
Device(config-if-vlan5)#end
```

Step 3: Configure AAA authentication.

#Enable AAA authentication on the Device, authentication method RADIUS, server key admin, priority 1, and RADIUS server address 130.255.167.167/24.

```
Device(config)#domain system
Device(config-isp-system)# aaa authentication dot1x radius-group radius
Device(config-isp-system)#exit
Device(config)#aaa server group radius radius
Device(config-rg-radius-radius)#server 130.255.167.167 priority 1 key admin
```

Step 4: Configure AAA server.

#On AAA server, configure user name, password and key value as admin. (Omitted)

Step 5: Configure secure channel.

#Enable secure channel access control on the port gigabitethernet 0/2.

```
Device#configure terminal
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#dot1x free-ip
Device(config-if-gigabitethernet0/2)#exit
```

#Configure a secure channel named channel, and configure to permit PC1 to access the Update Server, and PC2 to access both Update Server and IP Network.

```
Device#configure terminal
Device(config)#hybrid access-list advanced channel
Device (config-adv-hybrid-nacl)#permit ip any any host 199.0.0.10 any
Device(config-adv-hybrid-nacl)#permit ip host 199.0.0.2 any any any
```

#Apply the secure channel named channel.

```
Device#configure terminal
```

```
Device(config)#global security access-group channel
Device(config)#exit
```

Step 6: Check the result.

#View the configuration information of secure channel

```
Device#show dot1x free-ip
802.1X free-ip Enable Interface (num:1): gi0/2
global security access-group channel
Total free-ip user number : 0
```

```
Device#show hybrid access-list channel
hybrid access-list advanced channel
10 permit ip any any host 199.0.0.10 any
20 permit ip host 199.0.0.2 any any any
```

It is indicated that secure channel is enabled on gigabitethernet 0/2, and the secure channel rules of channel are bound.

#Before passing authentication, PC1 can access the Update Server instead of other network resources.

#After PC1 users initiate authentication and the authentication succeeds, view the information of user authentication.

```
Device#show dot1x user
```

```
-----
NO 1 : MAC_ADDRESS= 3883.45ef.7984 STATUS= Authorized USER_NAME= admin
      VLAN= 2 INTERFACE= gi0/2 USER_TYPE= DOT1X
      AUTH_STATE= AUTHENTICATED BACK_STATE= IDLE IP_ADDRESS= 199.0.0.1
      IPV6_ADDRESS= Unknown
```

```
Online time: 0 week 0 day 0 hours 0 minute 51 seconds
```

```
Total: 1 Authorized: 1 GetIP: 0 Unauthorized/guest/critical: 0/0/0 Unknown: 0
```

It is indicated that the PC1 user has passed authentication and can access the Update Server and IP Network.

#PC2 can access the Update Server and IP Network without authentication.

### 92.3.6 Configure IP Authorization as DHCP Server Mode

#### Network Requirements

- PC accesses IP network through the Device which enables 802.1X access control;
- RADIUS authentication is used as an authentication method;
- PC1 can access the IP Network after obtaining IP address through the specified DHCP Server;
- PC2 cannot access the IP Network after being configured with static IP address authentication.

## Network Topology

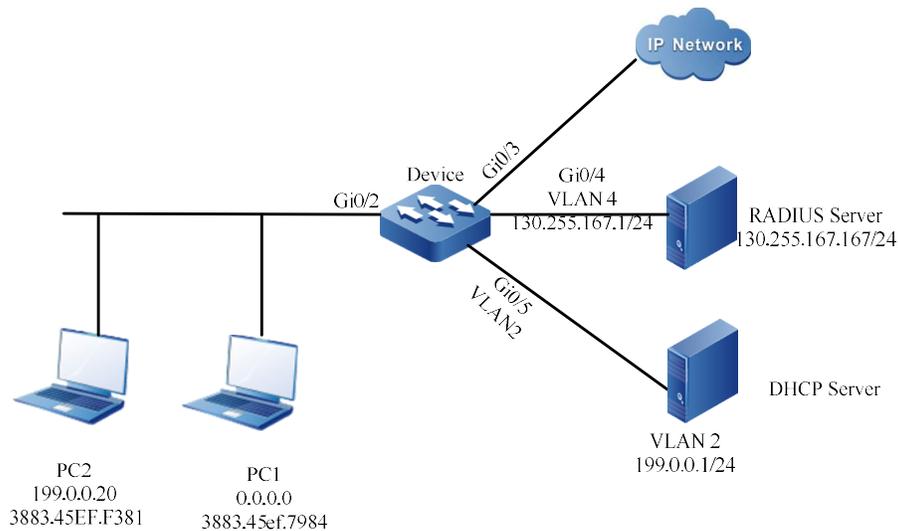


Figure 92 Network Topology for Configuring 802.1X IP Authorization as DHCP Server Mode

### Configuration Steps

Step 1: Configure VLAN and port link type on Device.

#On the Device, create VLAN2 and VLAN4, configure the link type of port as Hybrid on gigabitethernet0/2, permitting the services of VLAN2 to pass, and configure PVID as 2.

```
Device#configure terminal
Device(config)#vlan 2,4
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode hybrid
Device(config-if-gigabitethernet0/2)#switchport hybrid untagged vlan 2
Device(config-if-gigabitethernet0/2)#switchport hybrid pvid vlan 2
Device(config-if-gigabitethernet0/2)#exit
```

#Configure the link type of port as Access on gigabitethernet0/5 of the Device, allowing the services of VLAN2 to pass. (Omitted)

#Configure the link type of port as Access on gigabitethernet0/4 of the Device, allowing the services of VLAN4 to pass. (Omitted)

Step 2: Configure interface IP address for the Device.

#Configure the IP address of VLAN4 as 130.255.167.1/24.

```
Device(config)#interface vlan 4
Device(config-if-vlan4)#ip address 130.255.167.1 255.255.255.0
Device(config-if-vlan4)#exit
```

Step 3: Configure AAA authentication.

#Enable AAA authentication on the Device, authentication method RADIUS, server key admin, priority 1, and RADIUS server address 130.255.167.167/24.

```
Device(config)#domain system
Device(config-isp-system)# aaa authentication dot1x radius-group radius
Device(config-isp-system)#exit
Device(config)#aaa server group radius radius
Device(config-sg-radius-radius)#server 130.255.167.167 priority 1 key admin
```

Step 4: Configure AAA server.

#On AAA server, configure user name, password and key value as admin. (Omitted)

Step 5: Configure the DHCP server.

#Configure the segment of assigning IP address on the DHCP server as 199.0.0.2-199.0.0.10, and the subnet mask as 255.255.255.0. (omitted)

Step 6: On the Device, enable the DHCP Snooping function and configure gigabitethernet0/5 as a trusted port.

```
Device(config)#dhcp-snooping
Device(config)#intergice gigabitethernet 0/5
Device(config-if-gigabitethernet0/5)#dhcp-snooping trust
Device(config-if-gigabitethernet0/5)#exit
```

Step 7: Configure 802.1X authentication on the Device.

#Enable 802.1X authentication of gigabitethernet0/2.

```
Device(config)#intergice gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#dot1x port-control enable
Device(config-if-gigabitethernet0/2)#exit
```

#Configure the IP authorization of gigabitethernet0/2 as DHCP Server mode.

```
Device(config)#intergice gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#dot1x authorization ip-auth-mode dhcp-server
Device(config-if-gigabitethernet0/2)#exit
```

#Enable the ARP keepalive of gigabitethernet0/2.

```
Device(config)#intergice gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#dot1x client-probe enable
Device(config-if-gigabitethernet0/2)#exit
```

Step 8: Check the result.

#PC1 users can successfully pass the authentication and obtain IP address from DHCP server and access the IP Network.

```
Device#show dot1x user
```

User manual  
Release 1.0 01/2022

-----  
NO 1 : MAC\_ADDRESS= 3883.45ef.7984 STATUS= Authorized USER\_NAME= admin  
VLAN= 2 INTERFACE= gi0/2 USER\_TYPE= DOT1X  
AUTH\_STATE= AUTHENTICATED BACK\_STATE= IDLE IP\_ADDRESS= 199.0.0.3  
IPV6\_ADDRESS= Unknown

Online time: 0 week 0 day 0 hours 0 minutes 36 seconds

Total: 1 Authorized: 1 GetIP: 0 Unauthorized/guest/critical: 0/0/0 Unknown: 0

#PC2 users are under GET-IP status after authentication. They cannot obtain IP address.

NO 1 : MAC\_ADDRESS= 3883.45ef.f381 STATUS= Unauthorized USER\_NAME= admin  
VLAN= 2 INTERFACE= gi0/2 USER\_TYPE= DOT1X  
AUTH\_STATE= GET\_IP BACK\_STATE= IDLE IP\_ADDRESS= Unknown  
IPV6\_ADDRESS= Unknown

Online time: 0 week 0 day 0 hour 0 minute 34 seconds

Total: 1 Authorized: 0 GetIP: 0 Unauthorized/guest/critical: 1/0/0 Unknown: 0

#PC2 cannot access the IP Network even if it has passed authentication.

### 92.3.7 Configure 802.1X Critical VLAN

#### Network Requirements

- PC accesses IP network through the Device which enables 802.1X access control;
- RADIUS authentication is used as an authentication method;
- PC2 can access the Update Server only when it fails to pass authentication due to the unreachable server.

#### Network Topology

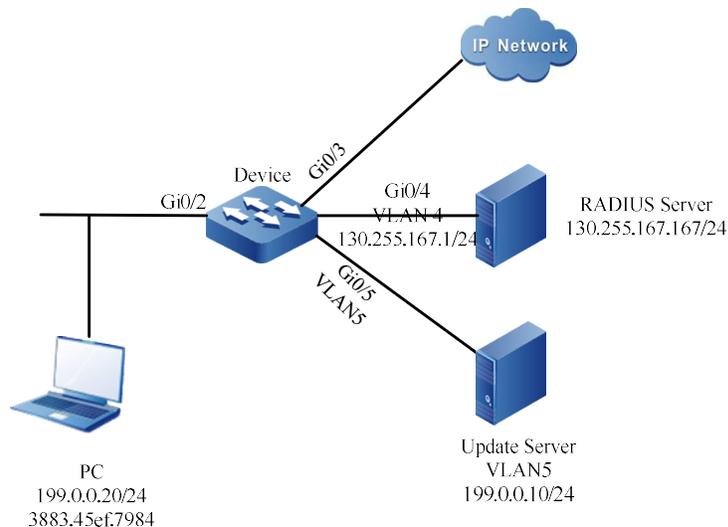


Figure 92 Network Topology for Configuring 802.1X Critical VLAN

## Configuration Steps

Step 1: Configure VLAN and port link type on Device.

#On the Device, create VLAN2, VLAN4 and VLAN5, configure the link type of port as Hybrid on gigabitethernet0/2, permitting the services of VLAN2 to pass, and configure PVID as 2.

```
Device#configure terminal
Device(config)#vlan 2,4,5
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode hybrid
Device(config-if-gigabitethernet0/2)#switchport hybrid untagged vlan 2
Device(config-if-gigabitethernet0/2)#switchport hybrid pvid vlan 2
Device(config-if-gigabitethernet0/2)#exit
```

#Configure the link type of port as Access on gigabitethernet0/5 of the Device, allowing the services of VLAN5 to pass. (Omitted)

#Configure the link type of port as Access on gigabitethernet0/4 of the Device, allowing the services of VLAN4 to pass. (Omitted)

Step 2: Configure interface IP address for the Device.

#Configure the IP address of VLAN4 as 130.255.167.1/24.

```
Device(config)#interface vlan 4
Device(config-if-vlan4)#ip address 130.255.167.1 255.255.255.0
Device(config-if-vlan4)#exit
```

Step 3: Configure AAA authentication.

#Enable AAA authentication on the Device, authentication method RADIUS, server key admin, priority 1, and RADIUS server address 130.255.167.167/24.

```
Device(config)#domain system
Device(config-isp-system)# aaa authentication dot1x radius-group radius
Device(config-isp-system)#exit
Device(config)#aaa server group radius radius
Device(config-sg-radius-radius)#server 130.255.167.167 priority 1 key admin
```

Step 4: Configure AAA server.

#On AAA server, configure user name, password and key value as admin. (Omitted)

Step 5: Configure 802.1X authentication on the Device.

#Enable 802.1X authentication of gigabitethernet 0/2.

```
Device(config)#interface gigabitethernet 0/2
User manual
Release 1.0 01/2022
```

```
Device(config-if-gigabitethernet0/2)#dot1x port-control enable
Device(config-if-gigabitethernet0/2)#exit
```

#Enable the MAC VLAN of gigabitethernet0/2.

```
Device(config)#intgigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#mac-vlan enable
Device(config-if-gigabitethernet0/2)#exit
```

#Configure the Critical VLAN of the port as VLAN5.

```
Device(config)#intgigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#authentication critical-vlan 5
Device(config-if-gigabitethernet0/2)#exit
```

Step 6: Check the result.

#The Device cannot ping the server when the server is abnormal. As a result, the user fails to pass authentication due to the unreachable server. The PC user is in the Critical VLAN and can access the Update Server.

Device#show dot1x user

```
-----
NO 1 : MAC_ADDRESS= 3883.45ef.7984 STATUS= Unauth(critical) USER_NAME= admin
      VLAN= 5 INTERFACE= gi0/2 USER_TYPE= DOT1X
      AUTH_STATE= CRITICAL_HELD BACK_STATE= IDLE IP_ADDRESS= Unknown
      IPV6_ADDRESS= Unknown
```

Total: 1 Authorized: 0 GetIP: 0 Unauthorized/guest/critical: 0/0/1 Unknown: 0

#At this time, the port gigabitethernet0/2 is added to the Critical VLAN.

Device#show vlan 5

```
-----
NO. VID VLAN-Name Owner Mode Intergice
-----
1 5 VLAN5 static Untagged gi0/2 gi0/5
```

### 92.3.8 Configure Combined Use of 802.1x and Port Security

#### Network Requirements

- PC accesses IP network through the Device which enables 802.1X access control and port security;
- RADIUS authentication is used as an authentication method;
- Configure port security rules that fail to match the MAC address of PC1, and PC1 can access the IP Network through authentication;
- Configure port security deny rules that fail to match the MAC address of PC2, and PC2 cannot pass authentication.

#### Network Topology

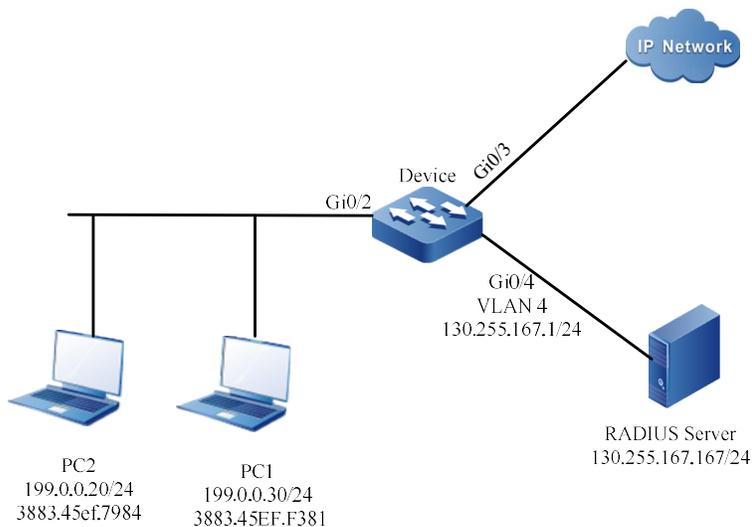


Figure 3 Network Topology for Configuring Combined Use of 802.1X and Port Security

### Configuration Steps

Step 1: Configure VLAN and port link type on Device.

#On the Device, create VLAN2 and VLAN4, configure the link type of port as Hybrid on gigabitethernet0/2, permitting the services of VLAN2 to pass, and configure PVID as 2.

```
Device#configure terminal
Device(config)#vlan 2,4
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode hybrid
Device(config-if-gigabitethernet0/2)#switchport hybrid untagged vlan 2
Device(config-if-gigabitethernet0/2)#switchport hybrid pvid vlan 2
Device(config-if-gigabitethernet0/2)#exit
```

#Configure the link type of port as Access on gigabitethernet0/4 of the Device, allowing the services of VLAN4 to pass. (Omitted)

Step 2: Configure interface IP address for the Device.

#Configure the IP address of VLAN4 as 130.255.167.1/24.

```
Device(config)#interface vlan 4
Device(config-if-vlan4)#ip address 130.255.167.1 255.255.255.0
Device(config-if-vlan4)#exit
```

Step 3: Configure AAA authentication.

#Enable AAA authentication on the Device, authentication method RADIUS, server key admin, priority 1, and RADIUS server address 130.255.167.167/24.

```
Device(config)#domain system
User manual
Release 1.0 01/2022
```

```
Device(config-isp-system)# aaa authentication dot1x radius-group radius
Device(config-isp-system)#exit
Device(config)#aaa server group radius radius
Device(config-sg-radius-radius)#server 130.255.167.167 priority 1 key admin
```

Step 4: Configure AAA server.

#On AAA server, configure user name, password and key value as admin. (Omitted)

Step 5: Configure 802.1X authentication on the Device.

#Enable 802.1X authentication of gigabitethernet0/2.

```
Device(config)#int gige gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#dot1x port-control enable
Device(config-if-gigabitethernet0/2)#exit
```

Step 6: Configure port security on the Device.

#On port gigabitethernet0/2, enable port security.

```
Device(config)#int gige gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#port-security enable
Device(config-if-gigabitethernet0/2)#exit
```

#Configure port security rules on port gigabitethernet0/2.

```
Device(config)#int gige gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#port-security deny mac-address 3883.45EF.7984
Device(config-if-gigabitethernet0/2)#exit
```

Step 7: Check the result.

#PC1 users can successfully pass the authentication and then access the IP Network.

```
Device#show dot1x user
```

-----

```
NO 1 : MAC_ADDRESS= 3883.45ef.f381 STATUS=   Authorized   USER_NAME=  admin
      VLAN=      2      INTERFACE=  gi0/2      USER_TYPE=  DOT1X
      AUTH_STATE= AUTHENTICATED  BACK_STATE= IDLE      IP_ADDRESS=  Unknown
      IPV6_ADDRESS= Unknown
```

```
Online time: 0 week 0 day 0 hour 0 minute 1 second
```

```
Total: 1  Authorized: 1  GetIP: 0  Unauthorized/guest/critical: 0/0/0  Unknown: 0
```

#PC2 users cannot successfully pass the authentication, so they cannot access the network.

# 93 PORTAL

## 93.1 Overview

### 93.1.1 Introduction

Portal authentication is often called Web authentication, i.e. accept the user name and password input by the user through Web pages to authenticate the user. Portal authentication technology offers a flexible access control method. It can realize access control in the access layer and key data entries that need to be protected without installing a client. Generally, Portal authentication website is called portal website.

When an unauthenticated user surfs on the Internet, the device forces the user to visit a specific site, i.e., the Portal server. The user can access the services therein for free without authentication, such as application (e.g. antivirus software and OS patches) upgrading. When the user needs to access other resources on the Internet, it must authenticate its identity on the Portal authentication page provided by the Portal server. It can access the network resources only when it passes authentication.

In addition to flexible authentication, Portal can provide convenient management function, and there is advertising, notification and other personalized services on the Portal authentication page.

### 93.1.2 System Composition of Portal

The typical networking method of Portal is shown in the figure below. It comprises four elements: Portal Client, Authentication Device, Portal Server and AAA Server (Authentication/Authorization/Accounting Server).

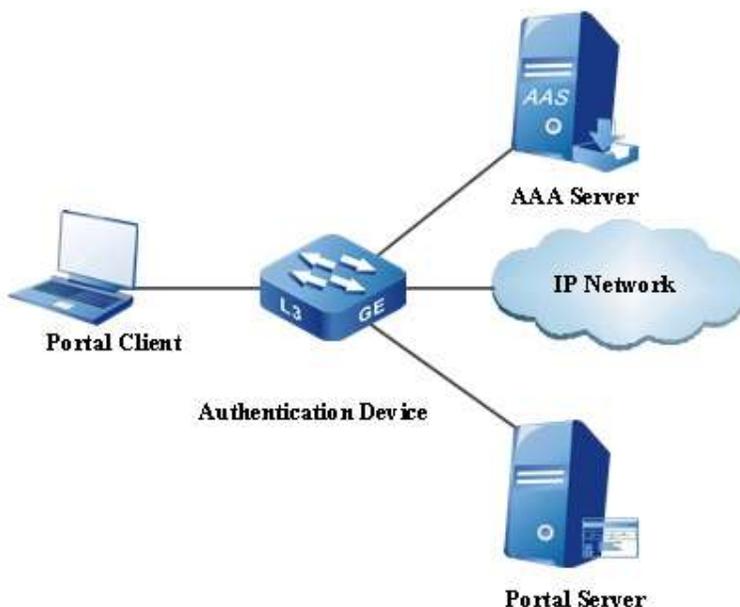


Figure 93 System Composition of Portal

- Portal Client: Generally the browser which runs HTTP or the proprietary Portal client software.
- Authentication Device: Located between the client and the authentication server, it controls network access of the client through interactions with Portal server and AAA server.
- Portal Server: The server system which receives authentication requests from the authentication client, and provides free portal service and Web authentication-based interface. After accepting the authentication requests from the authentication client and extracting authentication information therefrom, it interacts with the authentication device through the Portal protocol and notifies the authentication client of the authentication result.
- AAA Server: Generally, it is RADIUS (Remote Authentication Dial-In User Service) server. It is used to verify the legality of the client and notify the authentication result to the authentication device which controls network access of the client according to the authentication result.

### 93.1.3 Authentication Method of Portal

The Portal authentication method that can be used varies with networking mode. According to the network layer where Portal authentication is implemented in the network, Portal authentication method has two types, i.e. layer-2 authentication and layer-3 authentication.

#### 1. Layer-2 authentication

Support enabling the Portal authentication function on the layer-2 interface through which the authentication device connects with the user. Before authentication, the user obtains an IP address through manual configuration or DHCP, and can only access the Portal server; after passing the authentication, it can access network resources. Layer-2 authentication, based on source MAC control, permits the packets with legal source MAC address to pass after passing the authentication.

#### 2. Layer-3 authentication

Support enabling the Portal authentication function on the layer-3 interface through which the authentication device connects with the user. Layer-3 authentication has two types, i.e. general layer-3 authentication and secondary address allocation authentication.

##### (1) General layer-3 authentication

Before authentication, the user obtains an IP address through manual configuration or DHCP, and can only access the Portal server and the free access address set; after passing the authentication, it can access network resources. General layer-3 authentication realizes control in two ways:

- Based on source IP control, permitting the packets with legal source IP to

pass after passing the authentication.

- Based on source IP + source MAC control, permits the packets with legal source IP and source MAC address to pass after passing the authentication.

### 93.1.4 Authentication Process of Portal

There are two ways of authentication interaction between Portal server and authentication device:

- CHAP (Challenge Handshake Authentication Protocol): It is very secure as both user name and password are encrypted during transmission.
- PAP (Password Authentication Protocol): It has low security as both user name and password are transmitted in plaintext.

Portal server completes challenge handshake authentication through CHAP authentication interaction. Challenge is randomly generated by the authentication device when receiving Challenge request packets. With 16 bytes, it will be issued to the Portal server with Challenge response packets.

Layer-2 Portal authentication has the same process as general layer-3 Portal authentication.

#### 1. Process of layer-2 Portal and general layer-3 Portal authentication

The flow chart is shown below:

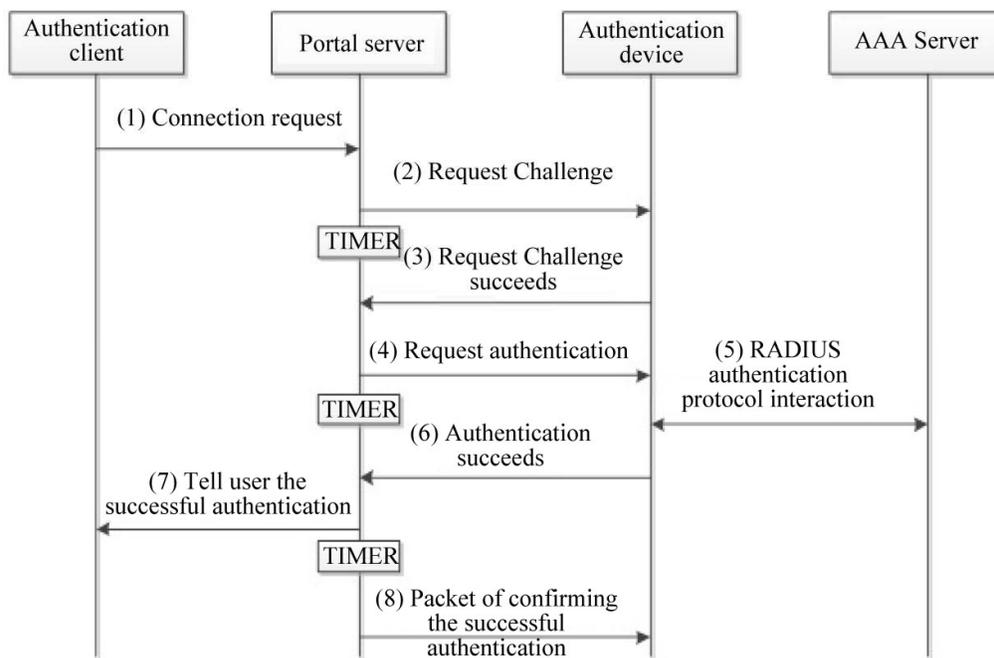


Figure 93 CHAP Flow Chart of Layer-2/General Layer-3 Portal Authentication

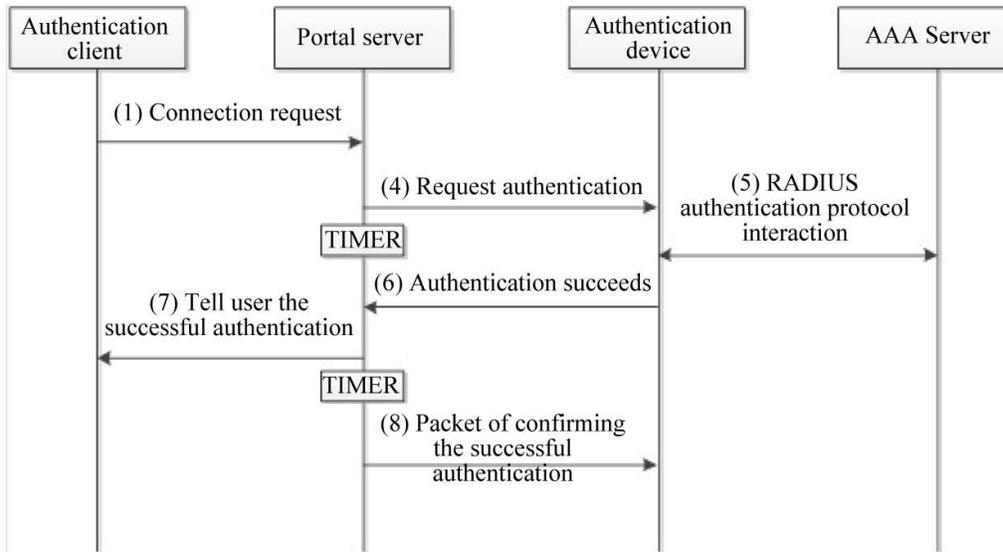


Figure 93 PAP Flow Chart of Layer-2/General Layer-3 Portal Authentication

Process of layer-2 Portal and general layer-3 Portal authentication:

- 1) Portal users have to initiate authentication requests when they need to access the network. When HTTP packets pass through the authentication device, the authentication device allows those accessing the Portal server or the free access address set to pass, and intercepts and redirects those accessing other addresses to the Portal server. The Portal server begins an authentication process by providing a Web page for users to input the legal user name and password that have been registered on the authentication server.
- 2) The Portal server uses CHAP authentication interaction to perform challenge handshake authentication. It will send a Challenge request to the authentication device. Use PAP authentication interaction to go to step (4).
- 3) The authentication device randomly generates a Challenge when receiving a Challenge request packet, and sends a successful challenge request packet to issue the Challenge to the Portal server. Use PAP authentication interaction to go to step (4).
- 4) The Portal server packets the user name and password input by the user into an authentication request packet and then sends it to the authentication device for authentication. At the same time, it enables the timer to wait for the authentication response.
- 5) The interaction of RADIUS protocol packets is conducted between the authentication device and the RADIUS server.
- 6) The authentication device sends a packet of successful authentication to the Portal server.
- 7) The Portal server sends the packet of successful authentication to the authentication

client to notify the user of the successful authentication.

- 8) The Portal server sends the packet of confirming successful authentication to the authentication device.

### 93.1.5 Support Issuing ACL

ACL (Access Control List) offers the function of controlling users' access to network resources and restricting users' access permission. When users go online, if an authorized ACL is configured on the server, the device will control the data flow of the port where the user is located according to the authorized ACL issued by the server; before configuring the authorized ACL on the server, it is required to configure corresponding rules on the device. Layer-2 Portal authentication supports issuing standard IP ACLs and extended IP ACLs; layer-3 Portal authentication supports issuing extended IP ACLs, and the matching items of the ACL rules configured support adding "source IP + source MAC".

## 93.2 Portal Function Configuration

Table 93 Portal Function Configuration List

Configuration Task	
Configure Portal Server and Attributes	Create Portal Server
	Configure Type of Portal Server
	Configure Detection Function for Portal Server
	Configure Source Interface for Sending Portal Packet
	Configure Destination UDP Port Number for Sending Packet of Forcing Users to Go Offline
Configure Layer-2 Portal Authentication Function	Enable Layer-2 Portal Authentication Function
Configure Layer-2 Portal Authentication Attributes	Configure Port Access Control Method
Configure Layer-3 Portal Authentication Function	Enable General Layer-3 Portal Authentication Function
	Configure and Apply Secure Channel

Configuration Task	
Configure Common Attributes	Configure the Maximum Number of Users on Interface
	Configure User Authentication Migration Function
	Configure the Function of Removing Domain Name
	Configure Timer Parameters
	Configure Authentication Method List
	Configure Accounting Method List

### 93.2.1 Configure Portal Server and Attributes

#### Configuration Condition

None

#### Create Portal Server

Create a Portal server and specify relevant parameters of the Portal server, including server IP address, shared encryption key, server port number, and server URL (authentication page address of the server).

Table 93 Creating Portal Server

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Create Portal Server	<b>portal server</b> <i>server-name</i> <b>ip</b> <i>ip-address</i> <b>key</b> [ <b>0</b>   <b>7</b> ] <i>key-string</i> [ <b>port</b> <i>udp-port-num</i>   <b>url</b> <i>url-string</i> ]	Optional By default, the Portal server is not created.



**Note**

- Portal authentication supports IPV4 protocol only.
- At most 5 Portal servers can be created on the authentication device.
- The parameters of the Portal server configured can be deleted or modified only when this Portal server is not referenced by interface.
- The shared keys configured on the authentication device and Portal server must be consistent.

### Configure Type of Portal Server

Configuring the type of Portal server is useful in two aspects:

- Different Portal servers extend the standard Portal protocol specifications.
- When no server URL is configured on the Portal server, it uses the default server URL of corresponding type for redirection.

The server types that can be specified include:

aas: AAS server, default server URL: http://IP-ADDRESS/portal/Login.do

imc: IMC server, default server URL: http://IP-ADDRES:8080/portal

user-defined: user-defined server, the default server URL format complies with the protocol specification "PORTAL Protocol Specification v2.0.2 for WLAN Service of China Mobile".

Table 93 Configuring Type of Portal Server

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure Type of Portal Server	<b>portal server <i>server-name</i> type { aas   imc   user-defined }</b>	Optional By default, the server type is AAS.

### Configure Detection Function for Portal Server

During the process of Portal authentication, if the communication between authentication device and Portal server is interrupted, new users cannot go online, and the Portal users who are already online cannot go offline normally. To solve this problem, the authentication device should be able to timely detect the changes of the reachable state of the Portal server, and trigger the performance of corresponding operation to respond to the influence of these changes. For example, when the specified Portal server is

unreachable, all users who use the Portal server for authentication will be forced to pass the authentication to access network resources, i.e. the Portal escape function.

Configure detection function so that the authentication device can detect the reachable state of the Portal server. The specific configurations are shown below:

- (1) Time interval of detecting reachability of server
- (2) Action performed when the reachable state of server changes
  - Log record: When the reachable state of Portal server changes, the log information is recorded.
  - Enable user restriction: When the reachable state of the Portal server changes, the log information is recorded; when the specified Portal server is unreachable, all users who use the Portal server for authentication will be forced to pass the authentication; when the Portal server is reachable again, the users who use this Portal server for forced authentication will be forced to go offline.

Table 93 Configuring Detection Function for Portal Server

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the time interval of detecting Portal server	<b>portal server</b> <i>server-name</i> <b>detect-interval</b> <i>detect-interval-value</i>	Optional By default, the time interval of detecting Portal server is 60 seconds, and the value range is 20~600 seconds or 0; when it is configured as 0, the Portal server cannot be detected.
Configure the action performed when the reachable state of the Portal server changes	<b>portal server</b> <i>server-name</i> <b>failover { log   permit }</b>	Optional By default, when the reachable state of Portal server changes, the log information is recorded.

### Configure Source Interface for Sending Portal Packet

Specify the source interface for sending Portal packet. The master IP address configured under the source interface is the source address used by the authentication device to send Portal packets to this Portal server. If there is no master IP address under the source interface, the communication will fail.

Table 93 Configuring Source Interface for Sending Portal Packet

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure Source Interface for Sending Portal Packet	<b>portal server</b> <i>server-name</i> <b>source-interface</b> <i>interface-name</i>	Optional By default, the source interface for sending Portal packet is not specified, and the user access interface is the source interface for sending Portal packet.

### Configure the Destination UDP Port Number for Sending Packet of Forcing Users to Go Offline

The port number of some servers for receiving the packet of forcing users to go offline is the specific UDP port number. Therefore, it's necessary to configure the destination UDP port number for sending packet of forcing users to go offline.

Table 93 Configuring Destination UDP Port Number for Sending Packet of Forcing Users to Go Offline

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the destination UDP port number for sending packet of forcing users to go offline	<b>portal server</b> <i>server-name</i> <b>ntf-logout-port</b> <i>udp-port-num</i>	Optional By default, the destination UDP port number for sending packet of forcing users to go offline is not specified. Instead, the port number of server is used.

## 93.2.2 Configure Layer-2 Portal Authentication Function

### Configuration Condition

To enable the layer-2 Portal authentication function, the following conditions should be met:

- This Portal server has been created on the authentication device

### Enable Layer-2 Portal Authentication Function

Enable layer-2 Portal authentication on the port of the authentication device connecting the user. The layer-2 authentication, based on source MAC control, permits the packets with legal source MAC address to pass after passing the authentication.

Table 93 Enabling Layer-2 Portal Authentication Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on current port.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the interface of current aggregation group.
Enable Layer-2 Portal Authentication Function	<b>portal server</b> <i>server-name</i> <b>method layer2</b>	Mandatory  By default, the layer-2 Portal authentication function under the port is disabled.

### Note

- The layer-2 Portal authentication doesn't support the issuance of VLAN.
- Layer-2 Portal authentication and Free-IP of 802.1X cannot be both configured for the same port.
- When layer-2 Portal authentication is enabled on the port, layer-3 Portal authentication cannot be enabled on corresponding VLAN interface. Otherwise, the configuration will fail.

- When the port where layer-2 Portal authentication is enabled is added to the VLAN interface where layer-3 Portal authentication is enabled, the configuration related to layer-2 Portal authentication of the port will be automatically cleared, and the log automatically cleared will be recorded.

### 93.2.3 Configure Layer-2 Portal Authentication Attributes

#### Configuration Condition

None

#### Configure Port Access Control Method

There are two types of port access control: Portbased and Macbased.

Portbased access control: Only one user is permitted to pass authentication under the port.

Macbased access control: Multiple users are permitted to pass authentication under the port. They cannot access the network without passing authentication.

The Portbased access control also has two modes: Multi-hosts and Single-host.

Multi-hosts: After one user passes authentication, other users under the port can access the network without authentication.

Single-host: Under the port, only one user is permitted to pass authentication and access the network. Other users cannot access the network or pass authentication.

Table 93-8 Configuring Port Access Control Method

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only on the

Step	Command	Description
		interface of current aggregation group.
Configure access control method	<b>authentication port-method { macbased   portbased }</b>	Mandatory By default, user authentication method is enabled under the port.
Portbased access control method	<b>authentication port-method portbased host-mode { multi-hosts   single-host }</b>	Optional By default, Multi-hosts authentication is enabled under the port.

---

### Note

- When configuring the host mode under portbased access control, you should guarantee that the access control method has been configured as Portbased.
- 

## 93.2.4 Configure Layer-3 Portal Authentication Function

### Configuration Condition

To enable the layer-3 Portal authentication function, the following conditions should be met:

- This Portal server has been created on the authentication device

### Enable General Layer-3 Portal Authentication Function

Enable the general layer-3 Portal authentication function on the layer-3 interface of the authentication device connecting to the user. The general layer-3 authentication has two control methods:

- Based on source IP control, permitting the packets with legal source IP to pass after passing the authentication.
- Based on source IP + source MAC control, permits the packets with legal source IP and source MAC address to pass after passing the authentication.

Table 93 Enabling General Layer-3 Portal Authentication Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Enable General Layer-3 Portal Authentication Function	<b>portal server</b> <i>server-name</i> <b>method layer3</b> [ <b>ip</b>   <b>ip-mac</b> ]	Mandatory  By default, the general layer-3 Portal authentication function of the interface is disabled.

---

### Note

- After the port under the general layer-3 Portal authentication interface is enabled, both 802.1X authentication and MAC authentication cannot be enabled.
  - After the port under the general layer-3 Portal authentication interface is enabled, the layer-2 Portal authentication function cannot be enabled.
  - When the port where layer-2 Portal authentication is enabled is added to the VLAN interface where the general layer-3 Portal authentication has been enabled, the enabling status of layer-2 Portal authentication is cleared.
- 

### Configure and Apply Secure Channel

After enabling the layer-3 authentication function under the layer-3 interface, to permit terminal users to access the resources in the specified network when they are not authenticated, or specify specific terminal users to access network resources without authentication, you need to configure and apply secure channel.

Secure channel rules can be configured as follows.

- Permit terminal users to access specified network resources.
- Permit specified terminal users to access network resources.

Table 1 Applying Secure Channel

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure secure channel	<b>hybrid access-list advanced</b> { <i>access-list-number</i>   <i>access-list-name</i> }	Mandatory  By default, no secure channel is configured in the device.
Configure secure channel rules	[ <i>sequence</i> ] <b>permit</b> <i>protocol</i> { <b>any</b>   <i>source-ip-addr</i> <i>source-wildcard</i>   <b>host</b> <i>source-ip-addr</i> } { <b>any</b>   <i>source-mac-addr</i> <i>source-wildcard</i>   <b>host</b> <i>source-mac-addr</i> } { <b>any</b>   <i>destination-ip-addr</i> <i>destination-wildcard</i>   <b>host</b> <i>destination-ip-addr</i> } { <b>any</b>   <i>destination-mac-addr</i> <i>destination-wildcard</i>   <b>host</b> <i>destination-mac-addr</i> }	Mandatory  By default, there are no secure channel rules under the secure channel.
Apply secure channel	<b>global security access-group</b> { <i>access-group-number</i>   <i>access-group-name</i> }	Mandatory  By default, no secure channel is applied in the system.

---

### Note

- A device can be configured with multiple secure channels, and a secure channel may have multiple secure channel rules.
  - The type of secure channel can be mixed advanced ACL only, and only one secure channel can be applied in the device.
- 

## 93.2.5 Configure Common Attributes

### Configuration Condition

None

2008

User manual  
Release 1.0 01/2022

## Configure the Maximum Number of Users on Interface

After the number of users authenticated under the interface reaches the upper limit configured, the authentication system no longer responds to the authentication request initiated by the new user.

The maximum number of users on layer-2 interface ranges from 1 to 4096, and that on layer-3 interface from 1 to 500.

Table 93 Configuring Maximum Number of Users on Interface

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	The subsequent configuration takes effect only on current interface after you enter the layer-2
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	Ethernet interface configuration mode, only on the interface of current aggregation group after you enter the aggregation group configuration mode, and only on current interface after you enter the interface configuration mode
Configure the Maximum Number of Users on Interface	<b>authentication max-user-num</b> <i>max-user-num-value</i>	Mandatory By default, at most 256 users are permitted to access under the interface.

---

### Note

- Under the layer-2 interface, configure as Macbased access control. Otherwise, the configured number of users permitted to access cannot take effect.
- 

## Configure User Authentication Migration Function

The user authentication migration function applies to the scenarios where the same user migrates from one authentication interface to another in the same device. When the user authentication migration function is disabled, after a user is authenticated on one interface of the device, it is not permitted to initiate authentication on another authentication interface of the device; when the user authentication migration function is enabled, after the user is authenticated on one interface, and the device finds that the user has migrated to another authentication interface, the device deletes the authentication information on the original interface and then permits the user to initiate authentication on a new authentication interface.

No matter whether the user authentication migration function is enabled, the device will record a log once it finds user migration between authentication interfaces.

Table 93 Configuring User Authentication Migration Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  The subsequent configuration takes effect only on current interface after you enter the layer-2 Ethernet interface configuration mode, only on the interface of current aggregation group after you enter the aggregation group configuration mode, and only on current interface after you enter the interface configuration mode
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	
Configure User Authentication Migration Function	<b>authentication station-move { enable   disable }</b>	Mandatory  By default, the user authentication migration function is disabled.

### Configure the Function of Removing Domain Name

In some scenarios, the username automatically contains the domain name when the client initiates authentication, and the user carrying the domain name cannot pass the authentication on the

authentication server. In order to avoid this, whether the authenticated user name sent to the authentication device contains a domain name can be configured for the authentication device.

Table 2 Configuring Function of Removing Domain Name

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  The subsequent configuration takes effect only on current interface after you enter the layer-2
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	Ethernet interface configuration mode, only on the interface of aggregation group after you enter the aggregation group configuration mode, and only on current interface after you enter the interface configuration mode
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	
Configure the Function of Removing Domain Name	<b>portal user-name-format</b> { <b>with-domain</b>   <b>without-domain</b> }	Mandatory  By default, the function of removing domain name is not configured.

### Configure Timer Parameters

The timer parameters under the interface include authenticating-period, authenticated-period, idle-period, and idle-period.

**Authenticating-period:** When any client packet is detected, the authenticating-period timer is enabled. After time-out of the timer, if no authentication result has been obtained, the client will be deleted.

**Authenticated-period:** After the client passes the authentication, this timer is enabled. After time-out of the timer, the information of the client which passes the authentication is deleted.

**Idle-period:** After the client passes the authentication, this timer is enabled. When the client is found offline, the information of the client which passes the authentication is deleted.

Quiet-period: When the client fails to pass the authentication, this timer is enabled. After time-out of the timer, the authentication device will respond to the authentication request from the client again.

The timer newly configure is valid for the authenticated users who later go online instead of those who have been online.

Table 3 Configuring Timer Parameters

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  The subsequent configuration takes effect only on current interface after you enter the layer-2 Ethernet interface configuration mode, only on the interface of current aggregation group after you enter the aggregation group configuration mode, and only on current interface after you enter the interface configuration mode
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	
Configure Timer Parameters	<b>portal timeout</b> { <b>authenticating-period</b> <i>authenticating-period-value</i>   <b>authenticated-period</b> <i>authenticated-period-value</i>   <b>idle-period</b> <i>idle-period-value</i>   <b>quiet-period</b> <i>quiet-period-value</i> }	Mandatory  By default,  the authenticating-period is 120 seconds, and the value range is 15~300;  the authenticated-period is 36000 seconds, and the value range is 0 or 300~864000;  the idle-period is 300 seconds, and the value range is 0 or 180~1800;  the quiet period is 60 seconds, and the value range is 15~3600.

### Configure Authentication Method List

Configure the authentication method list used by Portal users. When the user name of a Portal user contains a domain name, the authentication method list specified by the domain name is used; when there is no domain name in the Portal user name, the authentication method list configured is used.

Table 93 Configure Authentication Method List

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure to connect the authentication method list	<b>portal authentication method-list</b> { <b>default</b>   <i>list-name</i> }	Optional By default, the authentication method list of default is used.

### Configure Accounting Method List

The accounting method list used by Portal users. When the user name of a Portal user contains a domain name, the accounting method list specified by the domain name is used; when there is no domain name in the Portal user name, the accounting method list configured is used.

Table 4 Configuring Accounting Method List

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure to connect the accounting method list	<b>portal accounting method-list</b> { <b>default</b>   <i>list-name</i> }	Optional By default, the accounting method list of default is used.

## 93.2.6 Portal Monitoring and Maintaining

Table 93 Portal Monitoring and Maintaining

Command	Description
<b>clear portal user</b> { <b>ip</b> <i>ip-address</i>   <b>mac</b> <i>mac-address</i>   <b>all</b>   <b>interface</b> <i>interface-name</i>   <b>link-aggregation</b> <i>link-aggregation-id</i> }	Force the Portal user to go offline
<b>clear portal auth-fail-user history</b> [ <b>ip</b> <i>ip-address</i> ]	Clear record of failed authentication
<b>clear portal statistic</b> [ <b>interface</b> <i>interface-name</i>   <b>link-aggregation</b> <i>link-aggregation-id</i> ]	Clear authentication statistics
<b>show authentication user</b> [ <b>ip</b> <i>ip-address</i>   <b>mac</b> <i>mac-address</i>   <b>all</b>   <b>interface</b> <i>interface-name</i>   <b>link-aggregation</b> <i>link-aggregation-id</i>   <b>summary</b> ]	Show the information of authentication management users
<b>show authentication intf-status</b> [ <b>interface</b> <i>interface-name</i>   <b>link-aggregation</b> <i>link-aggregation-id</i> ]	Show the information of authentication status
<b>show portal</b>	Show default configurations of authentication
<b>show portal auth-fail-user history</b> [ <b>ip</b> <i>ip-address</i>   <b>recent</b> ]	Show the information of authentication failure
<b>show portal config</b> [ <b>interface</b> <i>interface-name</i>   <b>link-aggregation</b> <i>link-aggregation-id</i> ]	Show configurations of authentication
<b>show portal global config</b>	Show the information of global configuration
<b>show portal server</b>	Show the information of Portal server
<b>show portal statistic</b> [ <b>interface</b> <i>interface-name</i>   <b>link-aggregation</b> <i>link-aggregation-id</i> ]	Show authentication statistics
<b>show portal user</b> [ <b>ip</b> <i>ip-address</i>   <b>mac</b> <i>mac-address</i>   <b>interface</b> <i>interface-name</i>   <b>link-aggregation</b> <i>link-aggregation-id</i>   <b>summary</b> ]	Show user information

## 93.3 Typical Configuration Example of Portal

### 93.3.1 Configure Portbased Layer-2 Portal Authentication

#### Network Requirements

- PC1 and PC2 on the same LAN access the IP network through the Device where the layer-2 Portal authentication function is enabled and configured as Portbased.
- RADIUS authentication is used as an authentication method.
- Users can access the Portal Server only when they fail to pass authentication. They are permitted to access the IP Network once it passes the authentication.
- After one user on the LAN passes authentication, other users on this LAN can access the IP Network without authentication.

#### Network Topology

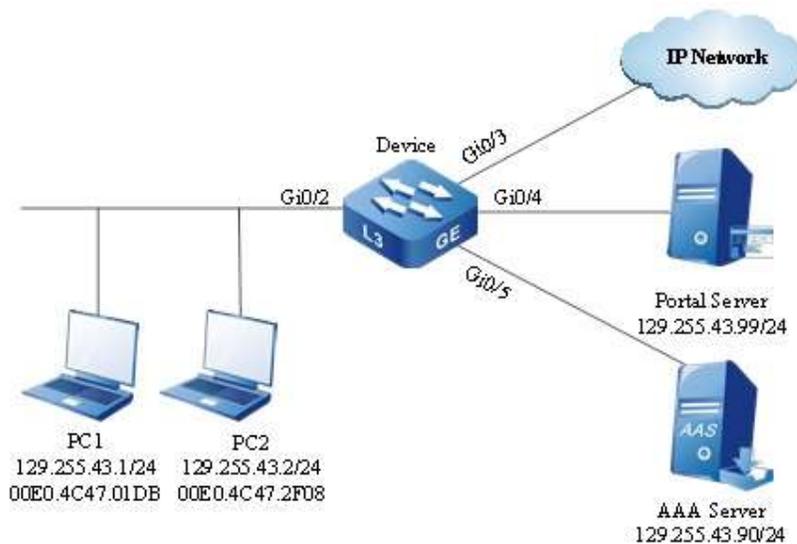


Figure 93 Network Topology for Configuring Portbased Layer-2 Portal Authentication

#### Configuration Steps

Step 1: Configure VLAN and port link type on Device.

#Create VLAN129 on the Device.

```
Device#configure terminal
Device(config)#vlan 129
Device(config)#exit
```

#Configure the link type of port gigabitethernet0/2 as Access, allowing the services of VLAN129 to pass.

```
Device(config)#interface gigabitethernet 0/2
```

```
Device(config-if-gigabitethernet0/2)#switchport mode access
Device(config-if-gigabitethernet0/2)#switchport access vlan 129
Device(config-if-gigabitethernet0/2)#exit
```

#Configure the link type of the ports gigabitethernet 0/3~gigabitethernet 0/5 on the Device as Access, allowing the services of VLAN129 to pass. (Omitted)

Step 2: Configure interface IP address for the Device.

#Configure the IP address of VLAN129 as 129.255.43.10/24.

```
Device(config)#interface vlan 129
Device(config-if-vlan129)#ip address 129.255.43.10 255.255.255.0
Device(config-if-vlan129)#exit
```

Step 3: Configure AAA authentication.

#Enable AAA authentication on the Device, authentication method RADIUS, RADIUS server address 129.255.43.90/24, server key admin, and priority 1.

```
Device#configure terminal
Device(config)#domain system
Device(config-isp-system)# aaa authentication portal radius-group radius
Device(config-isp-system)#exit
Device(config)#aaa server group radius radius
Device(config-sg-radius-radius)#server 129.255.43.90 priority 1 key admin
```

Step 4: Configure AAA server.

#On AAA server, configure user name, password and key value as admin. (Omitted)

Step 5: Configure layer-2 Portal authentication.

#On the Device, configure the Portal server of server1.

```
Device(config)# portal server server1 ip 129.255.43.99 key admin url http://129.255.43.99:8080/portal
```

#Enable layer-2 portal authentication on the Device and configure Portbased mode.

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#portal server server1 method layer2
Device(config-if-gigabitethernet0/2)#authentication port-method portbased
Device(config-if-gigabitethernet0/2)#exit
```

Step 6: Configure Portal server.

#On Portal server, configure IP address of PC1, address of the Device and key value as admin. (Omitted)

Step 7: Check the result.

#Before passing the authentication, PC1 and PC2 can access the Portal Server only.

#Verify that PC1 can pass the authentication. At this moment, both PC1 and PC2 can access the IP Network.

Device#show portal user

```
-----  
NO 1 : IP_ADDRESS= 129.255.43.1 STATUS= Authorized USER_NAME= admin  
      INTERFACE= gi0/2 CTRL_METHOD= L2_MAC AUTH_STATE= AUTHENTICATED  
      BACK_STATE= AAA_SM_IDLE VLAN= 129 MAC_ADDRESS= 00E0.4C47.01DB
```

Total: 1 Authorized: 1 Unauthorized/Guest/Critical: 0/0/0

### 93.3.2 Configure Macbased Layer-2 Portal Authentication

#### Network Requirements

- PC1 and PC2 on the same LAN access the IP network through the Device where the layer-2 Portal authentication function is enabled and configured as Macbased.
- RADIUS authentication is used as an authentication method.
- Users can access the Portal Server only when they fail to pass authentication. They are permitted to access the IP Network once it passes the authentication.
- After one user on the LAN passes authentication, it can access the IP Network. Other users on this LAN can access the IP Network only when they pass authentication.

#### Network Topology

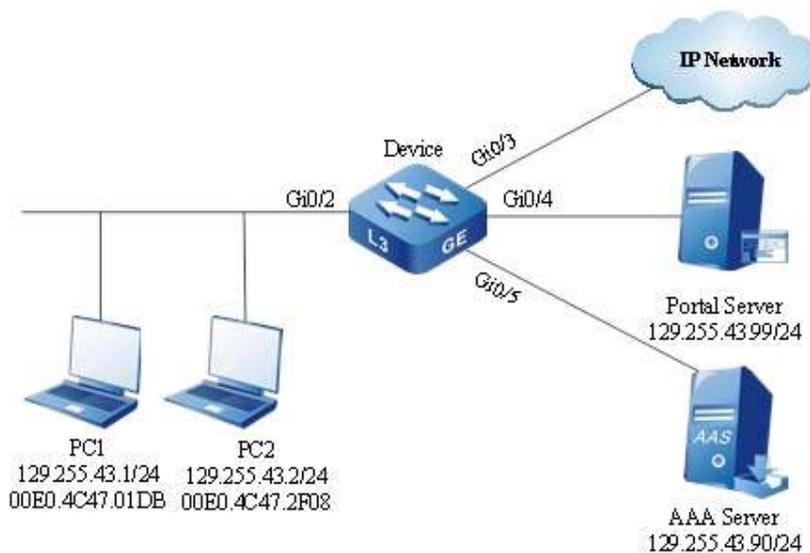


Figure 93 Network Topology for Configuring Macbased Layer-2 Portal Authentication

## Configuration Steps

Step 1: Configure VLAN and port link type on Device.

#Create VLAN129 on the Device.

```
Device#configure terminal
Device(config)#vlan 129
Device(config)#exit
```

#Configure the link type of port gigabitethernet0/2 as Access, allowing the services of VLAN129 to pass.

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode access
Device(config-if-gigabitethernet0/2)#switchport access vlan 129
Device(config-if-gigabitethernet0/2)#exit
```

#Configure the link type of the ports gigabitethernet 0/3~gigabitethernet 0/5 on the Device as Access, allowing the services of VLAN129 to pass. (Omitted)

Step 2: Configure interface IP address for the Device.

#Configure the IP address of VLAN129 as 129.255.43.10/24.

```
Device(config)#interface vlan 129
Device(config-if-vlan129)#ip address 129.255.43.10 255.255.255.0
Device(config-if-vlan129)#exit
```

Step 3: Configure AAA authentication.

#Enable AAA authentication on the Device, authentication method RADIUS, RADIUS server address 129.255.43.90/24, server key admin, and priority 1.

```
Device#configure terminal
Device(config)#domain system
Device(config-isp-system)# aaa authentication portal radius-group radius
Device(config-isp-system)#exit
Device(config)#aaa server group radius radius
Device(config-sg-radius-radius)#server 129.255.43.90 priority 1 key admin
```

Step 4: Configure AAA server.

#On AAA server, configure user name, password and key value as admin. (Omitted)

Step 5: Configure layer-2 Portal Authentication.

#On the Device, configure the Portal server of server1.

```
Device(config)# portal server server1 ip 129.255.43.99 key admin url http://129.255.43.99:8080/portal
```

#Enable layer-2 portal authentication on the Device and configure Macbased mode.

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#portal server server1 method layer2
Device(config-if-gigabitethernet0/2)#authentication port-method macbased
Device(config-if-gigabitethernet0/2)#exit
```

Step 6: Configure Portal server.

#On Portal server, configure IP address of PC1, address of the Device and key value as admin. (Omitted)

Step 7: Check the result.

#Before passing the authentication, PC1 and PC2 can access the Portal Server only.

#Verify that PC1 can pass the authentication. At this moment, PC1 instead of PC2 can access the IP Network.

```
Device#show portal user
```

```
-----
NO 1 : IP_ADDRESS= 129.255.43.1 STATUS= Authorized USER_NAME= admin
      INTERFACE= gi0/2 CTRL_METHOD= L2_MAC AUTH_STATE= AUTHENTICATED
      BACK_STATE= AAA_SM_IDLE VLAN= 129 MAC_ADDRESS= 00E0.4C47.01DB
      Total: 1 Authorized: 1 Unauthorized/Guest/Critical: 0/0/0
```

### 93.3.3 Configure General Layer-3 Portal Authentication

#### Network Requirements

- PC1 and PC2 on the same LAN access the IP network through the Device where the general layer-3 Portal authentication is enabled.
- RADIUS authentication is used as an authentication method.
- PC1 can access the Update Server only prior to passing authentication. It is permitted to access the IP Network once it passes the authentication.
- PC2 is permitted to access the Update Server.

#### Network Topology

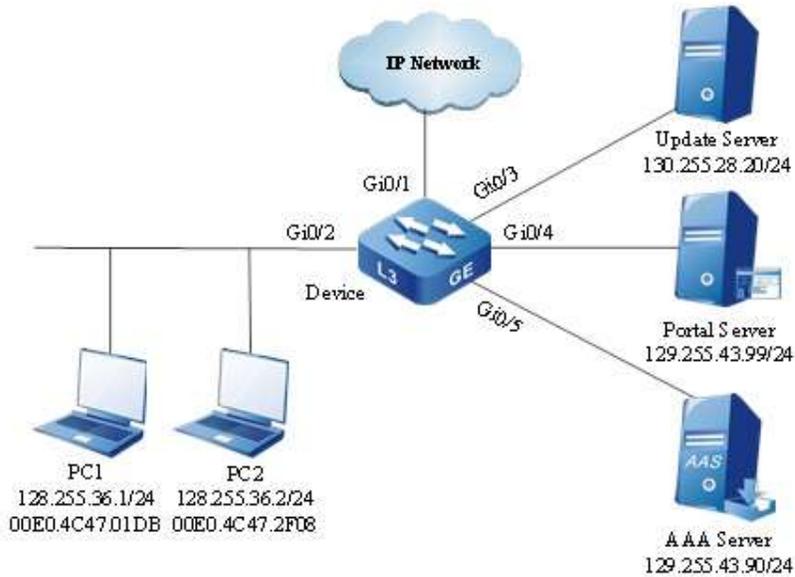


Figure 93 Network Topology for Configuring General Layer-3 Portal Authentication

### Configuration Steps

Step 1: Configure VLAN and link type on the port.

#Create VLAN128, VLAN129, VLAN130 and VLAN131 on the Device.

```
Device#configure terminal
Device(config)#vlan 128,129,130,131
Device(config)#exit
```

#Configure the link type of gigabitethernet0/2 to Access to allow services of VLAN128 to pass.

```
Device#configure terminal
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode access
Device(config-if-gigabitethernet0/2)#switchport access vlan 128
Device(config-if-gigabitethernet0/2)#end
```

#Configure the link type of port as Access on gigabitethernet 0/1 of the Device, allowing the services of VLAN131 to pass. Configure the link type of port as Access on gigabitethernet 0/3 of the Device to allow services of VLAN130 to pass, and as Access on gigabitethernet 0/4~gigabitethernet 0/5 to allow services of VLAN129 to pass. (Omitted)

Step 2: Configure interface IP address of the Device so that network routes are reachable.

#Configure the IP address of VLAN128 as 128.255.36.10/24.

```
Device#configure terminal
Device(config)#interface vlan 128
Device(config-if-vlan128)#ip address 128.255.36.10 255.255.255.0
```

```
Device(config-if-vlan128)#end
```

#Configure the IP address of VLAN129 as 129.255.43.10/24.

```
Device#configure terminal
```

```
Device(config)#interface vlan 129
```

```
Device(config-if-vlan129)#ip address 129.255.43.10 255.255.255.0
```

```
Device(config-if-vlan129)#end
```

#Configure the IP address of VLAN130 as 130.255.28.10/24.

```
Device#configure terminal
```

```
Device(config)#interface vlan 130
```

```
Device(config-if-vlan130)#ip address 130.255.28.10 255.255.255.0
```

```
Device(config-if-vlan130)#end
```

#Configure the IP address of VLAN131 as 131.255.28.10/24.

```
Device#configure terminal
```

```
Device(config)#interface vlan 131
```

```
Device(config-if-vlan131)#ip address 131.255.28.10 255.255.255.0
```

```
Device(config-if-vlan131)#end
```

Step 3: Configure AAA authentication.

#Enable AAA authentication on the Device, authentication method RADIUS, RADIUS server address 129.255.43.90/24, server key admin, and priority 1.

```
Device#configure terminal
```

```
Device(config)#domain system
```

```
Device(config-isp-system)#aaa authentication portal radius-group radius
```

```
Device(config-isp-system)#exit
```

```
Device(config)#aaa server group radius radius
```

```
Device(config-rg-radius-radius)#server 129.255.43.90 priority 1 key admin
```

Step 4: Configure AAA server.

#On AAA server, configure user name, password and key value as admin. (Omitted)

Step 5: Configure general layer-3 Portal authentication.

#On the Device, configure the Portal server of server1.

```
Device(config)#portal server server1 ip 129.255.43.99 key admin url http://129.255.43.99:8080/portal
```

#Enable layer-3 Portal authentication on the Device.

```
Device#configure terminal
```

```
Device(config)#interface vlan 128
```

```
Device(config-if-vlan128)#portal server server1 method layer3 ip
```

```
Device(config-if-vlan128)#exit
```

```
User manual
```

```
Release 1.0 01/2022
```

#Configure a secure channel named channel, and permit both PC1 and PC2 to access the Update Serve.

```
Device#configure terminal
Device(config)#hybrid access-list advanced channel
Device(config-adv-hybrid-nacl)#permit ip any any host 130.255.28.20 any
```

#Apply the secure channel named channel.

```
Device#configure terminal
Device(config)#global security access-group channel
Device(config)#exit
```

Step 6: Configure Portal server.

#On Portal server, configure IP address of PC1, address of the Device and key value as admin. (Omitted)

Step 7: Check the result.

#View the configuration information of secure channel

```
Device#show portal global config
```

```
portal global configuration information:
authentication method list : default
accounting method list    : default
```

```
global security access-group : channel
```

#Before passing authentication, PC1 can access the Update Server instead of IP Network.

#Verify that PC1 can pass the authentication. At this moment, PC1 can access both Update Server and IP Network; PC2 can access the Update Server instead of IP Network.

```
Device#show portal user
```

```
-----
NO 1:IP_ADDRESS= 128.255.36.1 STATUS=   Authorized   USER_NAME=  admin
      INTERFACE=  vlan128   CTRL_METHOD= L3_IP     AUTH_STATE= AUTHENTICATED
      BACK_STATE= AAA_SM_IDLE
```

```
Total: 1  Authorized: 1  Unauthorized/Guest/Critical: 0/0/0
```

# 94 Trusted Device Access

---

## 94.1 Overview

In order to prevent unauthorized access to the core network, the edge devices of core network must have high security. Therefore, other network devices that access these edge devices must be trusted ones. The trusted device access function implements the scheme of prohibiting unauthorized devices from accessing the core network based on the mature 802.1X protocol. Its basic network topology is shown in Figure 7-1. It includes three entities, i.e. Access Device, Authentication System and Authentication Server System.

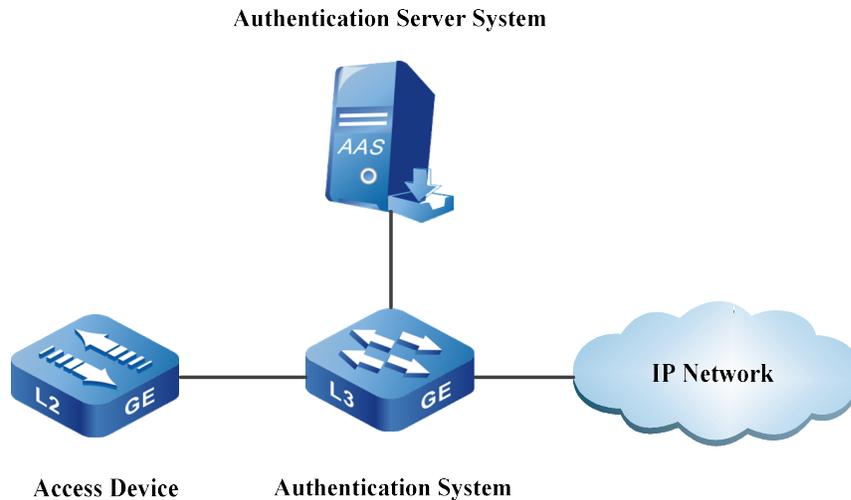


Figure 94 Topology for Trusted Device Access

The specific methods of accessing trusted device are shown below:

- Enable the trusted device access function on the access device, and configure the identity credential and relevant parameters required for device access on the access device and authentication server.
- Enable the authentication function of 802.1X device on the authentication device and make the port accessing to the access device become a controlled port for access of device.
- After the access device accesses the authentication device, it automatically initiates 802.1X authentication. After passing the 802.1X authentication, the authentication device turns on the controlled port to enable the access device to successfully access the network.
- The access device periodically conducts keepalive authentication according to the keepalive period set on the authentication device.

## 94.2 Configuration of Trusted Device Access

Table 94 Trusted Device Access Function Configuration List

Configuration Task	
Configure Trusted Device Access	Configure User Name and Password of Trusted Device Access
	Configure the User Name Format of Trusted Device Access
	Configure Trigger Period of Trusted Device Access
	Enable Trusted Device Access
Configure 802.1X Device Authentication	Enable 802.1X Device Authentication Function
	Configure Authentication Keepalive Period of 802.1X Device

## 94.2.1 Configure Trusted Device Access

### Configuration Condition

None

### Configure User Name and Password of Trusted Device Access

To successfully make the access device access the network, you are required to configure the user name and password of trusted device access on the port connecting the authentication device. The user name and password configured will be sent as the authentication credential of the access device to the authentication device for authentication through 802.1X protocol (MD5-Challenge mode).

Table 94 Configuring User Name and Password of Trusted Device Access

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the

Step	Command	Description
		current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Configure User Name and Password of Trusted Device Access	<b>dot1x client user</b> <i>username</i> <i>password 0 password</i>	Mandatory  By default, the user name and password of trusted device access are not configured under the port.

### Note

- Only one user name and password for device access can be configured under one port. The newly configured user name and password under the same port will overwrite the original ones under this port.

### Configure the User Name Format of Trusted Device Access

802.1X authentication identifies whether the peer end initiating authentication is device or terminal according to the device ID in the protocol packet EAP-Response/Identity. When the user name of the trusted device access under the port contains device ID, the authentication initiated by this port is 802.1X device authentication. When there is no device ID in the user name of the trusted device access under the port, the authentication initiated by this port is 802.1X terminal authentication.

Table 94 Configuring User Name Format of Trusted Device Access

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	

Step	Command	Description
		takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Configure the User Name Format of Trusted Device Access	<b>dot1x client user-name-format { with-dev-flag   without-dev-flag }</b>	Mandatory  By default, the user name of trusted device access under the port contains device ID.

#### Configure Trigger Period of Trusted Device Access

Before the access device passes the authentication, it actively sends an EAPoL-Start packet for 802.1X device authentication according to the access trigger period configured to ensure that the access device can quickly access the network.

Table 94 Configuring Trigger Period of Trusted Device Access

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	

Step	Command	Description
Configure Trigger Period of Trusted Device Access	<b>dot1x client auth-interval</b> <i>interval-value</i>	Mandatory  By default, the trigger period of trusted device access under the port is 15 seconds.

### Enable Trusted Device Access

After the device access function is enabled, the access device will actively conduct 802.1X device authentication prior to passing authentication. After passing the 802.1X authentication, the authentication device turns on the controlled port to enable the access device to successfully access the network.

Table 94 Enabling Trusted Device Access Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Enable Trusted Device Access	<b>dot1x client { enable   disable }</b>	Mandatory  By default, the trusted device access function under the port is disabled.

---

 **Note**

- The trusted device access and 802.1X authentication functions cannot be both enabled on the same port.
  - The trusted device access and MAC address authentication functions cannot be both enabled on the same port.
  - The trusted device access and secure channel authentication functions cannot be both enabled on the same port.
- 

## 94.2.2 Configure 802.1X Device Authentication

### Configuration Condition

None

### Enable 802.1X Device Authentication Function

To enable the 802.1X device authentication function to take effect on the authentication device, you are required to enable both 802.1X authentication and 802.1X device authentication function. After the authentication device takes effect, the port connecting authentication device and access device becomes a controlled one; after passing the authentication, the authentication device turns on the controlled port to enable the access device to successfully access the network.

Table 94 Enabling 802.1X Device Authentication Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected. After you enter the layer-2 Ethernet interface
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect

Step	Command	Description
		only within the aggregation group.
Enable 802.1X Authentication	<b>dot1x port-control { enable   disable }</b>	Mandatory By default, the 802.1X authentication function under the port is disabled.
Enable 802.1X device authentication	<b>dot1x device-auth { enable   disable }</b>	Mandatory By default, the 802.1X device authentication function under the port is disabled.

### Note

- The 802.1X device authentication and MAC address authentication functions cannot be both enabled on the same port.
- The 802.1X device authentication and secure channel authentication functions cannot be both enabled on the same port.

### Configure Authentication Keepalive Period of 802.1X Device

In order to check whether the access device is online, after passing the authentication, the authentication device sends the 802.1X device authentication keepalive period configured to the access device which initiates keepalive authentication with this keepalive period. If the authentication device fails to receive the keepalive authentication from the access device during a period which is three times the keepalive period, the access device is considered offline, and the port status is changed to controlled.

Table 94 Configuring Keepalive Period of 802.1X Device Authentication

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface <i>interface-name</i></b>	At least one option must be selected.

Step	Command	Description
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Configure Authentication Keepalive Period of 802.1X Device	<b>dot1x device-auth</b> <b>keepalive</b> <i>period-value</i>	Mandatory  By default, the keepalive period of 802.1X device authentication under the port is 600 seconds.

### 94.2.3 Trusted Device Access Monitoring and Maintaining

Table 94 Trusted Device Access Monitoring and Maintaining

Command	Description
<b>show dot1x client config</b> { <b>interface</b> <i>interface-name</i>   <b>link-aggregation</b> <i>link-aggregation-id</i> }	Show configuration information
<b>show dot1x client user</b> { <b>interface</b> <i>interface-name</i>   <b>link-aggregation</b> <i>link-aggregation-id</i> }	Shown access information
<b>show dot1x user</b> [ <i>mac-address</i>   <b>auth-type</b> { <b>device</b>   <b>user</b> }   <b>interface</b> <i>interface-name</i>   <b>link-aggregation</b> <i>link-aggregation-id</i>   <b>summary</b> ]	Show user information

## 94.3 Typical Configuration Example of Trusted Device Access

### Network Requirements

- The access device Device1 accesses the IP Network through the authentication device Device2 which uses device authentication access control.
- Device1 periodically initiates keepalive authentication.
- Use RADIUS authentication.
- After the access device passes authentication, PC can access the network.

### Network Topology

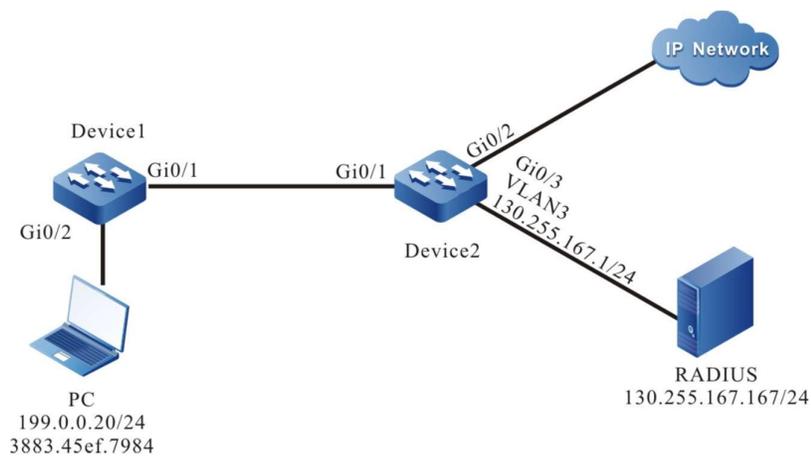


Figure 94 Network Topology for Configuring Trusted Device Access

### Configuration Steps

Step 1: Configure VLAN and port link type on Device1.

#Configure the link type of port as Access on gigabitethernet 0/2 of Device1, allowing the services of VLAN2 to pass.

```
Device1(config)#interface gigabitethernet 0/2
Device1(config-if-range)#switchport mode access
Device1(config-if-range)#switchport access vlan 2
Device1(config-if-range)#exit
```

#Configure the link type of port as Hybrid on gigabitethernet 0/1 of Device1, and add the port to VLAN2 in Tagged mode.

```
Device1(config)#interface gigabitethernet 0/1
Device1(config-if-range)#switchport mode hybrid
Device1(config-if-range)#switchport hybrid tagged vlan 2
Device1(config-if-range)#exit
```

Step 2: Configure VLAN and port link type on Device2.

#Create VLAN2-VLAN3 on Device2.

```
Device2#configure terminal
Device2(config)#vlan 2-3
Device2(config)#exit
```

#Configure the link type of port as Hybrid on gigabitethernet 0/1 of Device2, and add the port to VLAN2 in Tagged mode.

```
Device2(config)#interface gigabitethernet 0/1
Device2(config-if-range)#switchport mode hybrid
Device2(config-if-range)# switchport hybrid tagged vlan 2
Device2(config-if-range)#exit
```

#Configure the link type of port as Access on gigabitethernet 0/2~ gigabitethernet 0/3 of the Device2, allowing the services of VLAN2~VLAN3 to pass. (Omitted)

Step 3: Configure the interface IP address of Device2.

#Configure the IP address of VLAN3 as 130.255.167.1/24 on Device2.

```
Device2(config)#interface vlan 3
Device2(config-if-vlan3)#ip address 130.255.167.1 255.255.255.0
Device2(config-if-vlan3)#exit
```

Step 4: Configure AAA authentication on Device2.

#Enable AAA authentication on Device2, authentication method RADIUS, server key admin, priority 1, and RADIUS server address 130.255.167.167/24.

```
Device2(config)#aaa new-model
Device2(config)#aaa authentication connection default radius
Device2(config)#radius-server host 130.255.167.167 priority 1 key admin
```

Step 5: Configure AAA server.

#On AAA server, configure user name, password and key value as admin. (Omitted)

Step 6: Configure trusted device access on Device1.

#On Device1, configure the user name and password for trusted device access authentication.

```
Device1(config)#interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#dot1x client user admin password 0 admin
Device1(config-if-gigabitethernet0/1)#exit
```

#Configure to initiate eapol-start packet for 802.1X device authentication every 10 seconds.

```
Device1(config)#interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#dot1x client auth-interval 10
Device1(config-if-gigabitethernet0/1)#exit
```

#On Device1, enable the trusted device access function

```
Device1(config)#interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#dot1x client enable
Device2(config-if-gigabitethernet0/1)#exit
```

Step 7: Configure 802.1X device authentication on Device2.

#Enable 802.1X authentication on Device2.

```
Device2(config)#interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#dot1x port-control enable
Device2(config-if-gigabitethernet0/1)#exit
```

#Enable 802.1X device authentication on Device2

```
Device2(config)#interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#dot1x device-auth enable
Device2(config-if-gigabitethernet0/1)#exit
```

#On Device2, configure the keepalive period of 802.1X device authentication as 120 seconds.

```
Device2(config)#interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#dot1x device-auth keepalive 120
Device2(config-if-gigabitethernet0/1)#exit
```

Step 8: Check the result.

#Before the access device passes the authentication, PC cannot access the network. After passing authentication, PC can normally access the network.

```
Device1#show dot1x client user
Interface      : gi0/1
Status        : Authorized
State Machine State : AUTHENTICATED
Keep Alive Interval : 120 sec (802.1X Server)
```

```
Device2#show dot1x user auth-type device
```

```
-----
NO 1 : MAC_ADDRESS= 3883.45ef.7984  STATUS=   Authorized  USER_NAME=  admin
      VLAN=      2      INTERFACE=  gi0/1      USER_TYPE=  DOT1X
      AUTH_STATE= AUTHENTICATED  BACK_STATE= IDLE   IP_ADDRESS= Unknown
      Online time: 0 week 0 day 0 hour 0 minute 53 seconds
```

```
Total: 1 Authorized: 1 Unauthorized/guest/critical: 0/0/0 Unknown: 0
```

# 95 ACL Configuration

---

## 95.1 Overview

### 95.1.1 Overview

ACL (Access Control List) is composed of a series of rules. Each rule is a statement of permit, deny or comment, stating corresponding matching conditions and behaviors. ACL rules filter packets by matching some fields in the packets.

ACL can be composed of multiple rules. The matching content specified by each rule is not completely the same, and they may overlap or conflict. ACL rules match by numbers from small to large, and those with a small sequence number take effect first. Sequence means the sequence number of rules in the entire ACL.

Following the last ACL rule, there is a rule which denies all packets. Its sequence is larger than all the other rules. With this invisible rule, it will discard the packet which doesn't match all the prior rules. That is to say, when the packet doesn't match all the previous rules, the default rules will be matched and the packet will be discarded.

Depending on the application purpose, ACL can be divided into seven types, standard IP ACL, extended IP ACL, standard MAC ACL, extended MAC ACL, extended Hybrid ACL, standard IPv6 ACL, and extended IPv6 ACL. ACL name comprises figures or user-defined character strings. When figures are used as ACL name, corresponding ACL category and value range are shown below:

- Standard IP ACL: 1 ~ 1000;
- Extended IP ACL: 1001 ~ 2000;
- Standard MAC ACL: 2001 ~ 3000;
- Extended MAC ACL: 3001 ~ 4000;
- Extended hybrid ACL: 5001 ~ 6000;
- Standard IPv6 ACL: 6001 ~ 7000;
- Extended IPv6 ACL: 7001 ~ 8000;

When user-defined character strings are used as ACL name, all ACLs share the same space. That is to say, if standard IP ACL uses a certain name, other types of ACL cannot use this name again.

ACL can also perform corresponding action group according to the matching result. For details, see the chapters on "QOS Configuration" in the User Manual.

### 95.1.2 Time Domain

Time domain is a set of time periods. A time domain can contain multiple time periods, and the time scope of time domain is the union of all time periods.

Time period has two types:

- Periodic time period means one or several days from Monday to Sunday and the period from start time to end time are selected as time periods, which can repeatedly take effect per week;
- Absolute time period takes effect in the specified date and time scope.

Users often have the following requirements:

The PC in a certain network segment can access the server during the office hours of working days (except for all holidays); all PCs are permitted to communicate with external networks on Saturday afternoon;

These time-based communication control requirements can be satisfied by binding time domains in ACL or ACL rules.

## 95.2 ACL Function Configuration

Table 95 ACL Function Configuration List

Configuration Task	
Configure Standard IP ACL	Configure Standard IP ACL
	Configure Standard IP ACL Named with Figures
Configure Extended IP ACL	Configure Extended IP ACL
	Configure Extended IP ACL Named with Figures
Configure Standard MAC ACL	Configure Standard MAC ACL
	Configure Standard MAC ACL Named with Figures
Configure Extended MAC ACL	Configure Extended MAC ACL

Configuration Task	
	Configure Extended MAC ACL Named with Figures
Configure Extended Hybrid ACL	Configure Extended Hybrid ACL
	Configure Extended Hybrid ACL Named with Figures
Configure Standard IPv6 ACL	Configure Standard IPv6 ACL
	Configure Standard IPv6 ACL Named with Figures
Configure Extended IPv6 ACL	Configure Extended IPv6 ACL
	Configure Extended IPv6 ACL Named with Figures
Configure Limit of ACL Rule Entries	Configure Limit of ACL Rule Entries
Configure Time Domain	Configure Time Domain
	Configure Periodic Time Period
	Configure Absolute Time Period
	Configure Refresh Period
	Configure the Maximum Time Deviation
	Configure Binding of Time Domain to ACL Rules
	Configure Binding of Time Domain to ACL
Configure ACL Application	Configure Application of IP ACL to Port
	Configure Application of MAC ACL to Port
	Configure Application of IP ACL to VLAN
	Configure Application of IP ACL to Global
	Configure Global Application of Hybrid ACL
	Configure Application of IP ACL to Interface

Configuration Task	
	Configure Application of MAC ACL to Interface
	Configure Application of IPv6 ACL to Port
	Configure Application of IPv6 ACL to Interface

### 95.2.1 Configure Standard IP ACL

The standard IP ACL only filters packets according to the rules set by source IP address.

#### Configuration Condition

None

#### Configure Standard IP ACL

The standard IP ACL name comprises figures or user-defined character strings. When figures are used as standard IP ACL name, the maximum number of ACLs can be enabled; if user-defined character strings are used as standard IP ACL name, the maximum number of ACLs can be disabled. Users can choose an appropriate ACL name according to the actual situation.

Table 95 Configuring Standard IP ACL

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure Standard IP ACL	<b>ip access-list standard</b> { <i>access-list-number</i>   <i>access-list-name</i> }	Mandatory By default, no standard IP ACL is configured. Value range of standard IP ACL: 1 ~ 1000
Configure ACL permit rules	[ <i>sequence</i> ] <b>permit</b> { <b>any</b>   <i>source-addr source-wildcard</i>   <b>host</b> <i>source-addr</i> } [ <b>time-range</b> <i>time-range-name</i> ] [ <b>log</b> ]	Optional By default, no ACL permit rule is configured.

Step	Command	Description
	<pre>[ <b>pbr-action-group</b> pbr- action-group-name ]  [ <b>l3-action-group</b> l3-action- group-name ] [ <b>egr-action- group</b> egr-action-group- name ] [ <b>vfp-action-group</b> vfp-action-group-name ]</pre>	
Configure ACL deny rules	<pre>[ <i>sequence</i> ] <b>deny</b> { <b>any</b>   source-addr source- wildcard   <b>host</b> source- addr } [ <b>time-range</b> time- range-name ] [<b>log</b>]  [ <b>pbr-action-group</b> pbr- action-group-name ]  [ <b>l3-action-group</b> l3-action- group-name ] [ <b>egr-action- group</b> egr-action-group- name ] [ <b>vfp-action-group</b> vfp-action-group-name ]</pre>	Optional  By default, no ACL deny rule is configured.
Configure ACL comment	<pre>[ <i>sequence</i> ] <b>remark</b> comment</pre>	Optional  By default, no comment of ACL rules is configured.

---

## Note

- To create standard IP ACL with the command `ip access-list standard`, rules must be configured under the standard IP ACL configuration mode.
  - Sequence means the sequence number of rules in the entire ACL. ACLs match and filter packets by numbers from small to large, and those with a small sequence number take effect first. When the packet doesn't match any of the rules, the default discarding action will be performed, i.e. all the packets that have not been permitted to pass will be discarded.
- 

### Configure Standard IP ACL Named with Figures

The standard IP ACL rules named with figures allow users to quickly identify the type of ACL. But they have some limitations, such as limited number of access lists and complicated process for users to identify ACL rules.

Table 95 Configuring Standard IP ACL Named with Figures

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure Standard IP ACL Named with Figures	<b>access-list</b> <i>access-list-number</i> { <b>permit</b>   <b>deny</b> } { <b>any</b>   <i>source-addr source-wildcard</i>   <b>host</b> <i>source-addr</i> } [ <b>time-range</b> <i>time-range-name</i> ] [ <b>log</b> ] [ <b>pbr-action-group</b> <i>pbr-action-group-name</i> ] [ <b>l3-action-group</b> <i>l3-action-group-name</i> ] [ <b>egr-action-group</b> <i>egr-action-group-name</i> ] [ <b>vfp-action-group</b> <i>vfp-action-group-name</i> ]	Mandatory By default, no standard IP ACL named with figures is configured. Value range of standard IP ACL: 1 ~ 1000
Configure comment for standard IP ACL named with figures	<b>access-list</b> <i>access-list-number</i> <b>remark</b> <i>comment</i>	Optional By default, no comment for standard IP ACL rules named with figures is configured.

### Note

- If the ACL with a specified number doesn't exist, create a new ACL and add new rules. If the ACL with a specified number exists, add new rules only.

## 95.2.2 Configure Extended IP ACL

The extended IP ACL can set classification rules according to IP protocol number, source IP address, destination IP address, source TCP/UDP port number, destination TCP/UDP port number, packet priority, TCP flag, and fragment flag to filter the packets.

### Configuration Condition

None

## Configure Extended IP ACL

The extended ACL name comprises figures or user-defined character strings. When figures are used as extended IP ACL name, the maximum number of ACLs can be enabled; if user-defined character strings are used as extended IP ACL name, the maximum number of ACLs can be disabled. Users can choose an appropriate ACL name according to the actual situation. The extended IP ACL has more abundant, accurate and flexible content than standard IP ACL.

Table 95 Configuring Extended IP ACL

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure Extended IP ACL	<b>ip access-list extended</b> { <i>access-list-number</i>   <i>access-list-name</i> }	Mandatory  By default, no extended IP ACL is configured.  Value range of extended IP ACL: 1001 ~ 2000
Configure ACL permit rules	[ <i>sequence</i> ] <b>permit</b> <i>protocol</i> { <b>any</b>   <i>source-addr</i> <i>source-wildcard</i>   <b>host</b> <i>source-addr</i> } [ <i>operator</i> <i>source-port</i> ] { <b>any</b> / <i>destination-addr</i> <i>destination-wildcard</i>   <b>host</b> <i>destination-addr</i> } [ <i>operator</i> <i>destination-port</i> ] [ <b>ack</b>   <b>fin</b>   <b>psh</b>   <b>rst</b>   <b>syn</b>   <b>urg</b> ] [ <b>precedence</b> <i>precedence</i> ] [ <b>tos</b> <i>tos</i> ] [ <b>dscp</b> <i>dscp</i> ] [ <b>fragments</b> ] [ <b>log</b> ] [ <b>time-range</b> <i>time-range-name</i> ]  [ <b>pbr-action-group</b> <i>pbr-action-group-name</i> ]  [ <b>l3-action-group</b> <i>l3-action-group-name</i> ] [ <b>egr-action-group</b> <i>egr-action-group-name</i> ] [ <b>vfp-action-group</b> <i>vfp-action-group-name</i> ]	Optional  By default, no ACL permit rule is configured.

Step	Command	Description
Configure ACL deny rules	<pre>[ sequence ] deny protocol { any   source-addr source- wildcard   host source- addr } [ operator source- port ] { any   destination- addr destination-wildcard   host destination-addr } [ operator destination- port ] [ ack   fin   psh   rst   syn   urg ] [ precedence precedence ] [ tos tos ] [ dscp dscp ] [fragments] [log] [ time-range time- range-name ]  [ pbr-action-group pbr- action-group-name ]  [ l3-action-group l3-action- group-name ] [ egr-action- group egr-action-group- name ] [ vfp-action-group vfp-action-group-name ]</pre>	Optional By default, no ACL deny rule is configured.
Configure ACL comment	<pre>[ sequence ] remark comment</pre>	Optional By default, no comment of ACL rules is configured.

---

## Note

- To create extended IP ACL with the command **ip access-list extended**, rules must be configured under the extended IP ACL configuration mode.
  - Sequence means the sequence number of rules in the entire ACL. ACLs match and filter packets by numbers from small to large, and those with a small sequence number take effect first. When the packet doesn't match any of the rules, the default discarding action will be performed, i.e. all the packets that have not been permitted to pass will be denied.
- 

### Configure Extended IP ACL Named with Figures

The extended IP ACL rules named with figures allow users to quickly identify the type of ACL. But they have some limitations, such as limited number of access lists and complicated process for users to identify ACL rules. The extended IP ACL has more abundant, accurate and flexible content than standard IP ACL.

Table 95 Configuring Extended IP ACL Named with Figures

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure Extended IP ACL Named with Figures	<b>access-list</b> <i>access-list-number</i> { <b>permit</b>   <b>deny</b> } <i>protocol</i> { <b>any</b>   <i>source-addr</i> <i>source-wildcard</i>   <b>host</b> <i>source-addr</i> } [ <i>operator</i> <i>source-port</i> ] { <b>any</b> / <i>destination-addr</i> <i>destination-wildcard</i>   <b>host</b> <i>destination-addr</i> } [ <i>operator</i> <i>destination-port</i> ] [ <b>ack</b>   <b>fin</b>   <b>psh</b>   <b>rst</b>   <b>syn</b>   <b>urg</b> ] [ <b>precedence</b> <i>precedence</i> ] [ <b>tos</b> <i>tos</i> ] [ <b>dscp</b> <i>dscp</i> ] [ <b>fragments</b> ] [ <b>log</b> ] [ <b>time-range</b> <i>time-range-name</i> ]  [ <b>pbr-action-group</b> <i>pbr-action-group-name</i> ]  [ <b>l3-action-group</b> <i>l3-action-group-name</i> ] [ <b>egr-action-group</b> <i>egr-action-group-name</i> ] [ <b>vfp-action-group</b> <i>vfp-action-group-name</i> ]	Mandatory  By default, no extended IP ACL named with figures is configured.  Value range of extended IP ACL: 1001 ~ 2000
Configure comment for extended IP ACL named with figures	<b>access-list</b> <i>access-list-number</i> <b>remark</b> <i>comment</i>	Optional  By default, no comment for extended IP ACL rules named with figures is configured.

 **Note**

- If the ACL with a specified number doesn't exist, create a new ACL and add new rules. If the ACL with a specified number exists, add new rules only.

### 95.2.3 Configure Standard MAC ACL

The standard MAC ACL only filters packets according to the rules set by source MAC address.

#### Configuration Condition

None

#### Configure Standard MAC ACL

The standard MAC ACL name comprises figures or user-defined character strings. When figures are used as standard MAC ACL name, the maximum number of ACLs can be enabled; if user-defined character strings are used as standard MAC ACL name, the maximum number of ACLs can be disabled. Users can choose an appropriate ACL name according to the actual situation.

Table 95 Configuring Standard MAC ACL

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure Standard MAC ACL	<b>mac access-list standard</b> { <i>access-list-number</i>   <i>access-list-name</i> }	Mandatory  By default, no standard MAC ACL is configured.  Value range of standard MAC ACL: 2001 ~ 3000
Configure ACL permit rules	[ <i>sequence</i> ] <b>permit</b> { <b>any</b>   <i>source-addr source-wildcard</i>   <b>host</b> <i>source-addr</i> } [ <b>time-range</b> <i>time-range-name</i> ] [ <b>log</b> ] [ <b>I2-action-group</b> <i>I2-action-group-name</i> ] [ <b>egr-action-group</b> <i>egr-action-group-name</i> ] [ <b>vfp-action-group</b> <i>vfp-action-group-name</i> ]	Optional  By default, no ACL permit rule is configured.
Configure ACL deny rules	[ <i>sequence</i> ] <b>deny</b> { <b>any</b>   <i>source-addr source-wildcard</i>   <b>host</b> <i>source-addr</i> } [ <b>time-range</b> <i>time-range-name</i> ] [ <b>log</b> ] [ <b>I2-action-group</b> <i>I2-action-group-name</i> ] [ <b>egr-action-</b>	Optional  By default, no ACL deny rule is configured.

Step	Command	Description
	<b>group</b> <i>egr-action-group-name</i> ] [ <b>vfp-action-group</b> <i>vfp-action-group-name</i> ]	
Configure ACL comment	[ <i>sequence</i> ] <b>remark</b> <i>comment</i>	Optional By default, no comment of ACL rules is configured.

### Note

- To create standard MAC ACL with the command **mac access-list standard**, rules must be configured under the standard MAC ACL configuration mode.
- Sequence means the sequence number of rules in the entire ACL. ACLs match and filter packets by numbers from small to large, and those with a small sequence number take effect first. When the packet doesn't match any of the rules, the default discarding action will be performed, i.e. all the packets that have not been permitted to pass will be discarded.

### Configure Standard MAC ACL Named with Figures

The standard MAC ACL rules named with figures allow users to quickly identify the type of ACL. But they have some limitations, such as limited number of access lists and complicated process for users to identify ACL rules.

Table 95 Configuring Standard MAC ACL Named with Figures

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure Standard MAC ACL Named with Figures	<b>access-list</b> <i>access-list-number</i> { <b>permit</b>   <b>deny</b> } { <b>any</b>   <i>source-addr source-wildcard</i>   <b>host</b> <i>source-addr</i> } [ <b>time-range</b> <i>time-range-name</i> ] [ <b>log</b> ] [ <b>l2-action-group</b> <i>l2-action-group-name</i> ] [ <b>egr-action-group</b> <i>egr-action-group-name</i> ] [ <b>vfp-action-group</b> <i>vfp-action-group-name</i> ]	Mandatory By default, no standard MAC ACL named with figures is configured. Value range of standard MAC ACL: 2001 ~ 3000

Step	Command	Description
Configure comment for standard MAC ACL named with figures	<b>access-list</b> <i>access-list-number</i> <b>remark</b> <i>comment</i>	Optional By default, no comment for standard MAC ACL rules named with figures is configured.

## Note

- If the ACL with a specified number doesn't exist, create a new ACL and add new rules. If the ACL with a specified number exists, add new rules only.

### 95.2.4 Configure Extended MAC ACL

The extended MAC ACL can set classification rules according to Ethernet protocol type, source MAC address, destination MAC address, VLAN ID, and 802.1p priority to filter the packets.

#### Configuration Condition

None

#### Configure Extended MAC ACL

The extended MAC ACL name comprises figures or user-defined character strings. When figures are used as extended MAC ACL name, the maximum number of ACLs can be enabled; if user-defined character strings are used as extended MAC ACL name, the maximum number of ACLs can be disabled. Users can choose an appropriate ACL name according to the actual situation. The extended MAC ACL has more abundant, accurate and flexible content than standard MAC ACL.

Table 95 Configuring Extended MAC ACL

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure Extended MAC ACL	<b>mac access-list extended</b> { <i>access-list-number</i>   <i>access-list-name</i> }	Mandatory By default, no extended MAC ACL is configured.

Step	Command	Description
		Value range of extended MAC ACL: 3001 ~ 4000
Configure ACL permit rules	[ <i>sequence</i> ] <b>permit</b> { <b>any</b>   <i>source-addr source-wildcard</i>   <b>host</b> <i>source-addr</i> } { <b>any</b>   <i>destination-addr destination-wildcard</i>   <b>host</b> <i>destination-addr</i> } [ <b>ether-type</b> <i>type</i> ] [ <b>cos</b> <i>cos</i> ] [ <b>vlan-id</b> <i>vlan</i> ] [ <b>time-range</b> <i>time-range-name</i> ] [ <b>log</b> ] [ <b>l2-action-group</b> <i>l2-action-group-name</i> ] [ <b>egr-action-group</b> <i>egr-action-group-name</i> ] [ <b>vfp-action-group</b> <i>vfp-action-group-name</i> ]	Optional  By default, no ACL permit rule is configured.
Configure ACL deny rules	[ <i>sequence</i> ] <b>deny</b> { <b>any</b>   <i>source-addr source-wildcard</i>   <b>host</b> <i>source-addr</i> } { <b>any</b>   <i>destination-addr destination-wildcard</i>   <b>host</b> <i>destination-addr</i> } [ <b>ether-type</b> <i>type</i> ] [ <b>cos</b> <i>cos</i> ] [ <b>vlan-id</b> <i>vlan</i> ] [ <b>time-range</b> <i>time-range-name</i> ] [ <b>log</b> ] [ <b>l2-action-group</b> <i>l2-action-group-name</i> ] [ <b>egr-action-group</b> <i>egr-action-group-name</i> ] [ <b>vfp-action-group</b> <i>vfp-action-group-name</i> ]	Optional  By default, no ACL deny rule is configured.
Configure ACL comment	[ <i>sequence</i> ] <b>remark</b> <i>comment</i>	Optional  By default, no comment of ACL rules is configured.

## Note

- To create extended MAC ACL with the command **mac access-list extended**, rules must be configured under the extended MAC ACL configuration mode.

- Sequence means the sequence number of rules in the entire ACL. ACLs match and filter packets by numbers from small to large, and those with a small sequence number take effect first. When the packet doesn't match any of the rules, the default discarding action will be performed, i.e. all the packets that have not been permitted to pass will be discarded.

### Configure Extended MAC ACL Named with Figures

The extended MAC ACL rules named with figures allow users to quickly identify the type of ACL. But they have some limitations, such as limited number of access lists and complicated process for users to identify ACL rules. The extended MAC ACL has more abundant, accurate and flexible content than standard MAC ACL.

Table 95 Configuring Extended MAC ACL Named with Figures

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure Extended MAC ACL Named with Figures	<b>access-list</b> <i>access-list-number</i> { <b>permit</b>   <b>deny</b> } { <b>any</b>   <i>source-addr source-wildcard</i>   <b>host</b> <i>source-addr</i> } { <b>any</b>   <i>destination-addr destination-wildcard</i>   <b>host</b> <i>destination-addr</i> } [ <b>ether-type</b> <i>type</i> ] [ <b>cos</b> <i>cos</i> ] [ <b>vlan-id</b> <i>vlan</i> ] [ <b>time-range</b> <i>time-range-name</i> ] [ <b>log</b> ] [ <b>l2-action-group</b> <i>l2-action-group-name</i> ] [ <b>egr-action-group</b> <i>egr-action-group-name</i> ] [ <b>vfp-action-group</b> <i>vfp-action-group-name</i> ]	Mandatory  By default, no extended MAC ACL named with figures is configured.  Value range of extended MAC ACL: 3001 ~ 4000
Configure the comment for extended MAC ACL named with figures	<b>access-list</b> <i>access-list-number</i> <b>remark</b> <i>comment</i>	Optional  By default, no comment for extended MAC ACL rules named with figures is configured.



**Note**

- If the ACL with a specified number doesn't exist, create a new ACL and add new rules. If the ACL with a specified number exists, add new rules only.

### 95.2.5 Configure Extended Hybrid ACL

The extended Hybrid ACL can set classification rules according to source MAC address, destination MAC address, Ethernet Type, IP protocol number, source IP address, destination IP address, packet priority, VLAN ID and 802.1p priority to filter the packets.

#### Configuration Condition

None

#### Configure Extended Hybrid ACL

The extended Hybrid ACL name comprises figures or user-defined character strings. When figures are used as extended Hybrid ACL name, the maximum number of ACLs can be enabled; if user-defined character strings are used as extended Hybrid ACL name, the maximum number of ACLs can be disabled. Users can choose an appropriate ACL name according to the actual situation. The extended Hybrid ACL is more abundant, accurate and flexible content than that separately defined using IP ACL and MAC ACL.

Table 95 Configuring Extended Hybrid ACL

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure Extended Hybrid ACL	<b>hybrid access-list extended</b> { <i>access-list-number</i>   <i>access-list-name</i> }	Mandatory  By default, no extended Hybrid ACL is configured.  Value range of extended Hybrid ACL: 5001 ~ 6000
Configure ACL permit rules	[ <i>sequence</i> ] <b>permit</b> { <b>any</b>   <i>source-mac -addr source-wildcard</i>   <b>host</b> <i>source-mac-addr</i> } { <b>any</b>   <i>destination-mac-addr destination-wildcard</i>   <b>host</b> <i>destination-mac-addr</i> } [ <b>cos</b> <i>cos</i> ] [ <b>vlan-id</b> <i>vlan</i> ] [ <b>time-range</b> <i>time-range-name</i> ] [ <b>egr-action-</b>	Optional  By default, no ACL permit rule is configured.

Step	Command	Description
	<pre> <b>group</b> egr-action-group-name [ <b>I3-action-group</b> I3-action-group-name ] [<b>ether-type</b>] { etherne-type   ipv4 protocol } { <b>any</b>   source-ip-addr source-wildcard   <b>host</b> source-ip-addr } { <b>any</b>   destination-ip-addr destination-wildcard   <b>host</b> destination-ip-addr } [ <b>precedence</b> precedence ] [ <b>tos</b> tos ] [ <b>dscp</b> dscp ] [ <b>fragments</b> ] [ <b>time-range</b> time-range-name ] [<b>egr-action-group</b> egr-action-group-name] [ <b>I3-action-group</b> I3-action-group-name ] </pre>	
Configure ACL deny rules	<pre> [ <i>sequence</i> ] <b>deny</b> { <b>any</b>   source-mac -addr source-wildcard   <b>host</b> source-mac-addr } { <b>any</b>   destination-mac-addr destination-wildcard   <b>host</b> destination-mac-addr } [ <b>cos</b> cos ] [ <b>vlan-id</b> vlan ] [ <b>time-range</b> time-range-name ] [<b>egr-action-group</b> egr-action-group-name] [ <b>I3-action-group</b> I3-action-group-name ] [<b>ether-type</b>] { etherne-type   ipv4 protocol } { <b>any</b>   source-ip-addr source-wildcard   <b>host</b> source-ip-addr } { <b>any</b>   destination-ip-addr destination-wildcard   <b>host</b> destination-ip-addr } [ <b>precedence</b> precedence ] [ <b>tos</b> tos ] [ <b>dscp</b> dscp ] [ <b>fragments</b> ] [ <b>time-range</b> time-range-name ] [<b>egr-action-group</b> egr-action-group-name] [ <b>I3-action-group</b> I3-action-group-name ] </pre>	<p>Optional</p> <p>By default, no ACL deny rule is configured.</p>

Step	Command	Description
Configure ACL comment	[ <i>sequence</i> ] <b>remark</b> <i>comment</i>	Optional  By default, no comment of ACL rules is configured.

## Note

- To create extended Hybrid ACL with the command **hybrid access-list extended**, rules must be configured under the extended Hybrid ACL configuration mode.
- Sequence means the sequence number of rules in the entire ACL. ACLs match and filter packets by numbers from small to large, and those with a small sequence number take effect first. When the packet doesn't match any of the rules, the default discarding action will be performed, i.e. all the packets that have not been permitted to pass will be discarded.

### Configure Extended Hybrid ACL Named with Figures

The extended Hybrid ACL rules named with figures allow users to quickly identify the type of ACL. But they have some limitations, such as limited number of access lists and complicated process for users to identify ACL rules.

Table 95 Configuring Extended Hybrid ACL Named with Figures

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure Extended Hybrid ACL Named with Figures	<b>access-list</b> <i>access-list-number</i> { <b>permit</b>   <b>deny</b> } { <b>any</b>   <i>source-mac -addr source-wildcard</i>   <b>host</b> <i>source-mac-addr</i> } { <b>any</b>   <i>destination-mac-addr destination-wildcard</i>   <b>host</b> <i>destination-mac-addr</i> } [ <b>cos</b> <i>cos</i> ] [ <b>vlan-id</b> <i>vlan</i> ] [ <b>time-range</b> <i>time-range-name</i> ] [ <b>egr-action-group</b> <i>egr-action-group-name</i> ] [ <b>l3-action-group</b> <i>l3-action-group-name</i> ] [ <b>ether-type</b> { <i>ethernet-type</i>   <i>ipv4</i> }	Mandatory  By default, no extended Hybrid ACL named with figures is configured.  Value range of extended Hybrid ACL: 5001 ~ 6000

Step	Command	Description
	<i>protocol</i> } { <b>any</b>   <i>source-ip-addr</i> <i>source-wildcard</i>   <b>host</b> <i>source-ip-addr</i> } { <b>any</b>   <i>destination -ip-addr</i> <i>destination -wildcard</i>   <b>host</b> <i>destination-ip-addr</i> } [ <b>precedence</b> <i>precedence</i> ] [ <b>tos</b> <i>tos</i> ] [ <b>dscp</b> <i>dscp</i> ] [ <b>fragments</b> ] [ <b>time-range</b> <i>time-range-name</i> ] [ <b>egr-action-group</b> <i>egr-action-group-name</i> ] [ <b>l3-action-group</b> <i>l3-action-group-name</i> ]	
Configure the comment for extended Hybrid ACL named with figures	<b>access-list</b> <i>access-list-number</i> <b>remark</b> <i>comment</i>	Optional  By default, no comment for extended Hybrid ACL rules named with figures is configured.

### Note

- If the ACL with a specified number doesn't exist, create a new ACL and add new rules. If the ACL with a specified number exists, add new rules only.

## 95.2.6 Configure Standard IPv6 ACL

The standard IPv6 ACL can set classification rules according to the source IPv6 address field to filter the packets.

### Configuration Condition

None

### Configure Standard IPv6 ACL

The standard IPv6 ACL name comprises figures or user-defined character strings. When figures are used as standard IPv6 ACL name, the maximum number of ACLs can be enabled; if user-defined character strings are used as standard IPv6 ACL name, the maximum number of ACLs can be disabled. Users can choose an appropriate ACL name according to the actual situation.

Table 95 Configuring Standard IPv6 ACL

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure Standard IPv6 ACL	<b>ipv6 access-list standard</b> { <i>access-list-number</i>   <i>access-list-name</i> }	Mandatory  By default, no standard IPv6 ACL is configured.
Configure ACL permit rules	[ <i>sequence</i> ] <b>permit</b> { <b>any</b>   <i>source-addr/source-wildcard</i>   <b>host</b> <i>source-addr</i> } [ <b>time-range</b> <i>time-range-name</i> ]  [ <b>pbr-action-group</b> <i>pbr-action-group-name</i> ]  [ <b>I3-action-group</b> <i>I3-action-group-name</i> ] [ <b>egr-action-group</b> <i>egr-action-group-name</i> ]	Optional  By default, no ACL permit rule is configured.
Configure ACL deny rules	[ <i>sequence</i> ] <b>deny</b> { <b>any</b>   <i>source-addr/source-wildcard</i>   <b>host</b> <i>source-addr</i> } [ <b>time-range</b> <i>time-range-name</i> ] [ <b>I3-action-group</b> <i>I3-action-group-name</i> ] [ <b>egr-action-group</b> <i>egr-action-group-name</i> ] [ <b>pbr-action-group</b> <i>pbr-action-group-name</i> ]	Optional  By default, no ACL deny rule is configured.
Configure ACL comment	[ <i>sequence</i> ] <b>remark</b> <i>comment</i>	Optional  By default, no comment of ACL rules is configured.



**Note**

- To create standard IPv6 ACL with the command **ipv6 access-list standard**, rules must be configured under the standard IPv6 ACL configuration mode.
- Sequence means the sequence number of rules in the entire ACL. ACLs match and filter packets by numbers from small to large, and those with a small sequence number take effect first. When the packet doesn't match any of the rules, the default discarding action will be performed, i.e. all the packets that have not been permitted to pass will be denied.

### Configure Standard IPv6 ACL Named with Figures

The standard IPv6 ACL rules named with figures allow users to quickly identify the type of ACL. But they have some limitations, such as limited number of access lists and complicated process for users to identify ACL rules.

Table 95 Configuring Standard IPv6 ACL Named with Figures

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure Standard IPv6 ACL Named with Figures	<b>access-list access-list-number { permit   deny } { any   source-addr/source-wildcard   host source-addr } [ time-range time-range-name ] [ <b>l3-action-group</b> l3-action-group-name ] [ <b>egr-action-group</b> egr-action-group-name ] [ <b>pbr-action-group</b> pbr-action-group-name ]</b>	Mandatory  By default, no standard IPv6 ACL named with figures is configured.  Value range of standard IPv6 ACL: 6001 ~ 7000
Configure the comment for standard IPv6 ACL named with figures	<b>access-list access-list-number remark comment</b>	Optional  By default, no comment for standard IPv6 ACL rules named with figures is configured.

### Note

- If the ACL with a specified number doesn't exist, create a new ACL and add new rules. If the

---

ACL with a specified number exists, add new rules only.

---

## 95.2.7 Configure Extended IPv6 ACL

The extended IPv6 ACL can set classification rules according to IPv6 protocol number, source IPv6 address, destination IPv6 address, source TCP/UDP port number, destination TCP/UDP port number, packet priority, and TCP flag to filter the packets.

### Configuration Condition

None

### Configure Extended IPv6 ACL

The extended IPv6 ACL name comprises figures or user-defined character strings. When figures are used as extended IPv6 ACL name, the maximum number of ACLs can be enabled; if user-defined character strings are used as extended IPv6 ACL name, the maximum number of ACLs can be disabled. Users can choose an appropriate ACL name according to the actual situation.

Table 1 Configuring Extended IPv6 ACL

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure Extended IPv6 ACL	<b>ipv6 access-list extended</b> { <i>access-list-number</i>   <i>access-list-name</i> }	Mandatory By default, no extended IPv6 ACL is configured.
Configure ACL permit rules	[ <i>sequence</i> ] <b>permit protocol</b> { <b>any</b>   <i>source-addr/source-wildcard</i>   <b>host source-addr</b> } [ <i>operator source-port</i> ] { <b>any</b>   <i>destination-addr/destination-wildcard</i>   <b>host destination-addr</b> } [ <i>operator destination-port</i> ] [ <b>ack / fin / psh / rst / syn / urg</b> ] [ <b>precedence precedence</b> ] [ <b>tos tos</b> ] [ <b>dscp dscp</b> ] [ <b>fragments</b> ] [ <b>time-range time-range-name</b> ] [ <b>pbr-action-group pbr-action-group-name</b> ]	Optional By default, no ACL permit rule is configured.

Step	Command	Description
	[ <b>l3-action-group</b> <i>l3-action-group-name</i> ] [ <b>egr-action-group</b> <i>egr-action-group-name</i> ]	
Configure ACL deny rules	[ <i>sequence</i> ] <b>deny protocol</b> { <b>any</b>   <i>source-addr/source-wildcard</i>   <b>host</b> <i>source-addr</i> } [ <i>operator source-port</i> ] { <b>any</b>   <i>destination-addr/destination-wildcard</i>   <b>host</b> <i>destination-addr</i> } [ <i>operator destination-port</i> ] [ <b>ack</b> / <b>fin</b> / <b>psh</b> / <b>rst</b> / <b>syn</b> / <b>urg</b> ] [ <b>precedence</b> <i>precedence</i> ] [ <b>tos</b> <i>tos</i> ] [ <b>dscp</b> <i>dscp</i> ] [ <b>fragments</b> ] [ <b>time-range</b> <i>time-range-name</i> ] [ <b>pbr-action-group</b> <i>pbr-action-group-name</i> ]  [ <b>l3-action-group</b> <i>l3-action-group-name</i> ] [ <b>egr-action-group</b> <i>egr-action-group-name</i> ]	Optional  By default, no ACL deny rule is configured.
Configure ACL comment	[ <i>sequence</i> ] <b>remark</b> <i>comment</i>	Optional  By default, no comment of ACL rules is configured.

## Note

- To create extended IPv6 ACL with the command **ipv6 access-list extended**, rules must be configured under the extended IPv6 ACL configuration mode.
- Sequence means the sequence number of rules in the entire ACL. ACLs match and filter packets by numbers from small to large, and those with a small sequence number take effect first. When the packet doesn't match any of the rules, the default discarding action will be performed, i.e. all the packets that have not been permitted to pass will be denied.

### Configure Extended IPv6 ACL Named with Figures

The extended IPv6 ACL rules named with figures allow users to quickly identify the type of ACL. But they have some limitations, such as limited number of access lists and complicated process for users to identify ACL rules.

Table 2 Configuring Extended IPv6 ACL Named with Figures

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure Extended IPv6 ACL Named with Figures	<b>access-list</b> <i>access-list-number</i> { <b>permit</b>   <b>deny</b> } <i>protocol</i> { <b>any</b>   <i>source-addr/source-wildcard</i>   <b>host</b> <i>source-addr</i> } [ <i>operator source-port</i> ] { <b>any</b>   <i>destination-addr/destination-wildcard</i>   <b>host</b> <i>destination-addr</i> } [ <i>operator destination-port</i> ] [ <b>ack</b> / <b>fin</b> / <b>psh</b> / <b>rst</b> / <b>syn</b> / <b>urg</b> ] [ <b>precedence</b> <i>precedence</i> ] [ <b>tos</b> <i>tos</i> ] [ <b>dscp</b> <i>dscp</i> ] [ <b>fragments</b> ] [ <b>time-range</b> <i>time-range-name</i> ] [ <b>pbr-action-group</b> <i>pbr-action-group-name</i> ] [ <b>l3-action-group</b> <i>l3-action-group-name</i> ] [ <b>egr-action-group</b> <i>egr-action-group-name</i> ]	Mandatory  By default, no extended IPv6 ACL named with figures is configured.  Value range of extended IPv6 ACL: 7001 ~ 8000
Configure the comment for extended IPv6 ACL named with figures	<b>access-list</b> <i>access-list-number</i> <b>remark</b> <i>comment</i>	Optional  By default, no comment for extended IPv6 ACL rules named with figures is configured.

## Note

- If the ACL with a specified number doesn't exist, create a new ACL and add new rules. If the ACL with a specified number exists, add new rules only.

### 95.2.8 Configure Commit operation

Commit operating command is used to confirm the ACL rules configured, including whether the rules added or deleted take effect. After an ACL rule is added or deleted, Commit operation must be performed. Otherwise, the rule added or deleted will not take effect. When the configuration is saved, the added rule without Committing will not be saved to the Startup file.

#### Configuration Condition

## Configure ACL

### Configure Commit operation

After an ACL rule is configured, it is required to perform Commit operation to commit current ACL rule added or deleted.

Table 95 Configuring Commit Operation for ACL Rules

Step	Command	Description
Enter the ACL configuration mode	<b>ip access-list standard</b> { <i>access-list-number</i>   <i>access-list-name</i> }	Mandatory  By default, no standard IP ACL is configured.  Value range of standard IP ACL: 1 ~ 1000  The ACL configuration mode is not limited to standard IP ACL. Commit operation supports all the ACL configuration modes.
Commit ACL rules	<b>commit</b>	Mandatory  By default, the rule added or deleted is not Committed.

### 95.2.9 Configure Limit of ACL Rule Entries

#### Configuration Condition

None

#### Configure Limit of ACL Rule Entries

After it is enabled, at most 1024 rule entries can be configured in a single ACL.

Table 95 Configuring Limit of ACL Rule Entries

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Disable/enable the limit of ACL rule entries	<b>access-list rule-limit</b> { <b>enable</b>   <b>disable</b> }	Mandatory  By default, this function is disabled, i.e. the number of rule entries configured in each ACL is not limited by the maximum number 1024.

### 95.2.10 Configure Time Domain

Time domain is a set of time periods. A time domain can contain multiple time periods, and the time scope of time domain is the union of all time periods. Time domain can be bound to ACL or ACL rule as a precondition for the ACL or ACL rule to take effect or not.

#### Configuration Condition

Before configuring the time domain function, do the following:

- Configure the ACL.

#### Configure Time Domain

Configure whether the application object of time domain is limited by the time domain. When it is enabled, all application objects are limited by time domain. Otherwise, they are not limited by time domain.

Table 3 Configuring Time Domain

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure to enable/disable time domain	<b>set time-range</b> { <b>disable</b>   <b>enable</b> }	Mandatory  It is enabled by default.

#### Configure Periodic Time Period

Periodic time period means one or several days from Monday to Sunday and the period from start time to end time are selected as time periods, which can repeatedly take effect per week.

Table 4 Configuring Periodic Time Period

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure Time Domain	<b>time-range</b> <i>time-range-name</i>	Mandatory By default, time domain is not configured.
Configure Periodic Time Period	[ <i>sequence</i> ] <b>periodic</b> [ <i>day-of-the-week</i> ] [ <i>hh: mm</i> [ : <i>ss</i> ] ] <b>to</b> [ <i>day-of-the-week</i> ] [ <i>hh: mm</i> [ : <i>ss</i> ] ]	At least one option must be selected. By default, no periodic time period is configured.
	[ <i>sequence</i> ] <b>periodic</b> { <b>weekdays</b>   <b>weekend</b>   <b>daily</b> } [ <i>hh: mm</i> [ : <i>ss</i> ] ] <b>to</b> [ <i>hh: mm</i> [ : <i>ss</i> ] ]	The previous command can specify the time scope as a single day (e.g. Monday) or several days (Monday, Friday). The latter command can specify the time scope as every day, weekend, or working days.

### Configure Absolute Time Period

Absolute time period takes effect in the specified date and time scope.

Table 95 Configuring Absolute Time Period

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure Time Domain	<b>time-range</b> <i>time-range-name</i>	Mandatory By default, time domain is not configured.
Configure absolute time period of time domain	[ <i>sequence</i> ] <b>absolute start</b> <i>hh: mm</i> [ : <i>ss</i> ] [ <i>day</i> [ <i>month</i> [ <i>year</i> ] ] ] <b>end</b> <i>hh: mm</i> [ : <i>ss</i> ] [ <i>day</i> [ <i>month</i> [ <i>year</i> ] ] ]	Mandatory By default, the absolute time period of time domain is not configured.

## Configure Refresh Period

Time domain has two statuses, i.e. valid and invalid. By default, it automatically refreshes every 1 minute according to current system time. Therefore, the status refresh may have 0-60 seconds of time delay compared to the system time.

Table 95 Configuring Refresh Period

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure time domain refresh period	<b>set time-range frequency</b> { <i>frequency-min</i>   <b>seconds</b> <i>frequency-sec</i> }	Mandatory  The default value is 1 minute.  The refresh period is the interval between two refreshes, in minute or second.

## Configure the Maximum Time Deviation

The maximum time deviation means the maximum deviation between the accumulated time of the counter and the system time. Once the time statistics exceed the deviation value, the status of each time domain will be judged and updated at the time of next refreshing so as to get increasingly accurate time statistics.

Table 5 Configuring Maximum Time Deviation

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the maximum time deviation of time domain	<b>set time-range max-offset</b> <i>max-offset-number</i>	Mandatory  The default value is 100.  The time deviation, in seconds, has a value range of 1~300.

## Configure Binding of Time Domain to ACL Rules

When it's necessary to make a user access network resources during a specified period of time, you can set the time domain-based ACL rules to filter packets. Whether the time domain takes effect has a direct impact on the ACL rules associated with it.

Table 6 Configuring Binding of Time Domain to ACL Rules

Step	Command	Description
Configure to bind with standard IP ACL rules	Please see "Configure Standard IP ACL"	-
Configure to bind with extended IP ACL rules	Please see "Configure Extended IP ACL"	-
Configure to bind with standard MAC ACL rules	Please see "Configure Standard MAC ACL"	-
Configure to bind with extended MAC ACL rules	Please see "Configure Extended MAC ACL"	-
Configure to bind with extended Hybrid ACL rules	Please see "Configure Extended Hybrid ACL"	-
Configure to bind with standard IPv6 ACL rules	Please see "Configure Standard IPv6 ACL"	-
Configure to bind with extended IPv6 ACL rules	Please see "Configure Extended IPv6 ACL"	-

---

### Note

- When the time domain to which ACL rules are bound doesn't exist, the ACL rules take effect.
- 

## Configure Binding of Time Domain to ACL

When it's necessary to make some users access network resources during the same period of time, you can set the time domain-based ACL to filter packets. Whether the time domain takes effect has a direct impact on the rules contained in the entire ACL.

Table 7 Configuring Binding of Time Domain to ACL

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure binding of time domain to IP ACL	<b>ip time-range</b> <i>time-range-name</i> <b>access-list</b> { <i>access-list-number</i>   <i>access-list-name</i> }	Mandatory By default, the time domain is not bound to IP ACL.
Configure binding of time domain to MAC ACL	<b>mac time-range</b> <i>time-range-name</i> <b>access-list</b> { <i>access-list-number</i>   <i>access-list-name</i> }	Mandatory By default, the time domain is not bound to MAC ACL.
Configure binding of time domain to Hybrid ACL	<b>hybrid time-range</b> <i>time-range-name</i> <b>access-list</b> { <i>access-list-number</i>   <i>access-list-name</i> }	Mandatory By default, the time domain is not bound to Hybrid ACL.
Configure binding of time domain to IPv6 ACL	<b>ipv6 time-range</b> <i>time-range-name</i> <b>access-list</b> { <i>access-list-number</i>   <i>access-list-name</i> }	Mandatory By default, the time domain is not bound to IPv6 ACL.

---

## Note

- When the time domain to which ACL is bound doesn't exist, the ACL takes effect.
- 

### 95.2.11 Configure ACL Application

ACL can be applied globally, in VLAN, VLAN RANGE, port and interface. MAC ACL, IP ACL and IPV6 ACL can all be applied to VLAN, VLAN RANGE, port and interface in both incoming and outgoing directions; Hybrid ACL can be applied to global, port and interface in both incoming and outgoing directions; IP ACL can be applied to global in the incoming direction;

When ACL is applied globally, it will filter all packets in the incoming direction of the device port; when ACL is applied to VLAN, it will filter all packets in the incoming direction and the forwarded packets in the outgoing direction of the port in the VLAN; when ACL is applied to VLAN RANGE, it will take effect for VLANs within the VLAN RANGE; when ACL is applied to a port, all packets in the incoming direction and the

forwarded packets in the outgoing direction of the port will be filtered; when ACL is applied to an interface, the layer-3 forwarded packets will be filtered.

ACL matches by priority from high to low: apply to port, apply to VLAN, and apply globally.

If the packets simultaneously match the ACL rules of applying to port, applying to VLAN and applying globally, the permitted packet with a high priority is matched first, and the packet with a filtering result of deny is directly discarded.

### Configuration Condition

Before configuring ACL application, do the following:

- Configure the ACL.

### Configure Application of IP ACL to Port

Apply IP ACL to the port to analyze and process the packets passing through this port according to the IP ACL.

Table 95 Configuring Application of IP ACL to Port

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the L2/L3 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2/3 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Configure to apply IP ACL to port	<b>ip access-group</b> { <i>access-list-number</i>   <i>access-list-name</i> } { <b>in</b>   <b>out</b>   <b>vfp</b> }	Mandatory  By default, no IP ACL is applied to the port.

---

 **Note**

- If the ACL applied to port doesn't exist, all the packets passing through this port will be permitted.
- 

### Configure Application of IPv6 ACL to Port

Apply IPv6 ACL to the port to analyze and process the packets passing through this port according to the IPv6 ACL.

Table 8 Configuring Application of IPv6 ACL to Port

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the L2/L3 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2/3 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>link-aggregation</b> <i>link-aggregation-id</i>	
Configure to apply IPv6 ACL to port	<b>ipv6 access-group</b> { <i>access-list-number</i>   <i>access-list-name</i> } { <b>in</b>   <b>out</b> }	Mandatory  By default, no IPv6 ACL is applied to the port.

---

 **Note**

- If the ACL applied to port doesn't exist, all the packets passing through this port will be permitted.
-

## Configure Application of MAC ACL to Port

Apply MAC ACL to the port to analyze and process the packets passing through this port according to the MAC ACL.

Table 9 Configuring Application of MAC ACL to Port

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the L2/L3 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2/3 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Configure to apply MAC ACL to port	<b>mac access-group</b> { <i>access-list-number</i>   <i>access-list-name</i> } { <b>in</b>   <b>out</b>   <b>vfp</b> }	Mandatory  By default, no MAC ACL is applied to the port.

---

### Note

- If the ACL applied to port doesn't exist, all the packets passing through this port will be permitted.
- 

## Configure Application of HYBRID ACL to Port

Apply HYBRID ACL to the port to analyze and process the packets passing through this port according to the HYBRID ACL.

Table 10 Configuring Application of HYBRID ACL to Port

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the L2/L3 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	After you enter the layer-2/3 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Configure to apply HYBRID ACL to port	<b>hybrid access-group</b> { <i>access-list-number</i>   <i>access-list-name</i> } { <b>in</b>   <b>out</b> }	Mandatory  By default, no HYBRID ACL is applied to the port.

### Configure Application of IP ACL to VLAN

Apply IP ACL to VLAN to analyze and process the packets passing through this VLAN according to the IP ACL.

Table 11 Configuring Application of IP ACL to VLAN

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the VLAN configuration mode	<b>vlan</b> <i>vlan-id</i>	-
Configure to apply IP ACL to VLAN	<b>ip access-group</b> { <i>access-list-number</i>   <i>access-list-name</i> } { <b>in</b>   <b>out</b>   <b>vfp</b> }	Mandatory  By default, no IP ACL is applied to VLAN.

---

 **Note**

- If the ACL applied to VLAN doesn't exist, all the packets passing through this VLAN will be permitted.
- 

### Configure Application of MAC ACL to VLAN

Apply MAC ACL to VLAN to analyze and process the packets passing through this VLAN according to the MAC ACL.

Table 12 Configuring Application of MAC ACL to VLAN

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the VLAN configuration mode	<b>vlan</b> <i>vlan-id</i>	-
Configure to apply MAC ACL to VLAN	<b>mac access-group</b> { <i>access-list-number</i>   <i>access-list-name</i> } { <b>in</b>   <b>out</b> }	Mandatory By default, no MAC ACL is applied to VLAN.

---

 **Note**

- If the ACL applied to VLAN doesn't exist, all the packets passing through this VLAN will be permitted.
- 

### Configure Application of IPv6 ACL to VLAN

Apply IPv6 ACL to VLAN to analyze and process the packets passing through this VLAN according to the IPv6 ACL.

Table 13 Configuring Application of IPv6 ACL to VLAN

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Enter the VLAN configuration mode	<b>vlan</b> <i>vlan-id</i>	-
Configure to apply IPv6 ACL to VLAN	<b>ipv6 access-group</b> { <i>access-list-number</i>   <i>access-list-name</i> } { <b>in</b>   <b>out</b> }	Mandatory By default, no IPv6 ACL is applied to VLAN.

### Note

- If the ACL applied to VLAN doesn't exist, all the packets passing through this VLAN will be permitted.

### Configure Application of MAC ACL to VLAN RANGE

Apply MAC ACL to VLAN RANGE to analyze and process the packets passing within this VLAN RANGE according to the MAC ACL.

Table 14 Configuring Application of MAC ACL to VLAN RANGE

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure to apply MAC ACL to VLAN RANGE	<b>mac access-group</b> { <i>access-list-number</i>   <i>access-list-name</i> } { <b>in</b>   <b>out</b> } <b>vlan range</b> <1-4094>	Mandatory By default, no MAC ACL is applied to VLAN RANGE.

### Note

- If the ACL applied to VLAN RANGE doesn't exist, all the packets passing through this VLAN RANGE will be permitted.

### Configure Application of IP ACL to VLAN RANGE

Apply IP ACL to VLAN RANGE to analyze and process the packets passing within this VLAN RANGE according to the IP ACL.

Table 15 Configuring Application of IP ACL to VLAN RANGE

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure to apply IP ACL to VLAN RANGE	<b>ip access-group</b> { <i>access-list-number</i>   <i>access-list-name</i> } { <b>in</b>   <b>out</b> } <b>vlan range</b> <1-4094>	Mandatory By default, no IP ACL is applied to VLAN RANGE.

### Note

- If the ACL applied to VLAN RANGE doesn't exist, all the packets passing through this VLAN RANGE will be permitted.

### Configure Application of IPv6 ACL to VLAN RANGE

Apply IPv6 ACL to VLAN RANGE to analyze and process the packets passing within this VLAN RANGE according to the IPv6 ACL.

Table 16 Configuring Application of IPv6 ACL to VLAN RANGE

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure to apply IPv6 ACL to VLAN RANGE	<b>ipv6 access-group</b> { <i>access-list-number</i>   <i>access-list-name</i> } { <b>in</b>   <b>out</b> } <b>vlan range</b> <1-4094>	Mandatory By default, no IPv6 ACL is applied to VLAN RANGE.

### Note

- If the ACL applied to VLAN RANGE doesn't exist, all the packets passing through this VLAN RANGE will be permitted.

### Configure Application of MAC ACL to VLAN RANGE of layer-3 interface

Apply MAC ACL to VLAN RANGE of layer-3 interface to analyze and process the packets passing within this VLAN RANGE of layer-3 interface according to the MAC ACL.

Table 17 Configuring Application of MAC ACL to VLAN RANGE of Layer-3 Interface

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure application of MAC ACL to VLAN RANGE of layer-3 interface	<b>mac access-group</b> { <i>access-list-number</i>   <i>access-list-name</i> } { <b>in</b>   <b>out</b> } <b>interface</b> <b>vlan range</b> <1-4094>	Mandatory By default, no MAC ACL is applied to VLAN RANGE of layer-3 interface.

### Note

- If the ACL applied to VLAN RANGE of layer-3 interface doesn't exist, all the packets passing through this VLAN RANGE will be permitted.

### Configure Application of IP ACL to VLAN RANGE of layer-3 interface

Apply IP ACL to VLAN RANGE of layer-3 interface to analyze and process the packets passing within this VLAN RANGE of layer-3 interface according to the IP ACL.

Table 18 Configuring Application of IP ACL to VLAN RANGE of Layer-3 Interface

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure application of IP ACL to VLAN RANGE of layer-3 interface	<b>ip access-group</b> { <i>access-list-number</i>   <i>access-list-name</i> } { <b>in</b>   <b>out</b> } <b>interface</b> <b>vlan range</b> <1-4094>	Mandatory By default, no IP ACL is applied to VLAN RANGE of layer-3 interface.

### Note

- If the ACL applied to VLAN RANGE of layer-3 interface doesn't exist, all the packets passing through this VLAN RANGE will be permitted.

### Configure Application of IPv6 ACL to VLAN RANGE of layer-3 interface

Apply IPv6 ACL to VLAN RANGE of layer-3 interface to analyze and process the packets passing within this VLAN RANGE of layer-3 interface according to the IPv6 ACL.

Table 19 Configuring Application of IPv6 ACL to VLAN RANGE of Layer-3 Interface

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure application of IPv6 ACL to VLAN RANGE of layer-3 interface	<b>ipv6 access-group</b> { <i>access-list-number</i>   <i>access-list-name</i> } { <b>in</b>   <b>out</b> } <b>interface vlan range</b> <1-4094>	Mandatory By default, no IPv6 ACL is applied to VLAN RANGE of layer-3 interface.

#### Note

- If the ACL applied to VLAN RANGE of layer-3 interface doesn't exist, all the packets passing through this VLAN RANGE will be permitted.

### Configure Application of IP ACL to Global

Apply IP ACL globally to analyze and process the packets passing through all ports according to the IP ACL.

Table 20 Configuring Global Application of IP ACL

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure to apply IP ACL globally	<b>global ip access-group</b> { <i>access-list-number</i>   <i>access-list-name</i> } <b>in</b>	Mandatory By default, no IP ACL is applied globally.

#### Note

- If the ACL applied globally doesn't exist, and no ACL is set on all ports, all the packets

---

passing through the port will be permitted.

---

### Configure Global Application of Hybrid ACL

Apply Hybrid ACL globally to analyze and process the packets passing through all ports according to the Hybrid ACL.

Table 21 Configuring Global Application of Hybrid ACL

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure to apply Hybrid ACL globally	<b>global hybrid access-group</b> { <i>access-list-number</i>   <i>access-list-name</i> } { <b>in</b>   <b>out</b> }	Mandatory  By default, no Hybrid ACL is applied globally.

---

### Note

- If the ACL applied globally doesn't exist, and no ACL is set on all ports, all the packets passing through all ports will be permitted.
- 

### Configure Application of IP ACL to Interface

Apply IP ACL to interface to analyze and process the packets passing through this interface according to the IP ACL.

Table 22 Configuring Application of IP ACL to Interface

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-

Step	Command	Description
Configure to apply IP ACL to interface	<b>ip access-group</b> { <i>access-list-number</i>   <i>access-list-name</i> } { <b>in</b>   <b>out</b> }	Mandatory  By default, no IP ACL is applied to the interface.

### Note

- If the ACL applied to interface doesn't exist, all the packets passing through this interface will be permitted.

### Configure Application of MAC ACL to Interface

Apply MAC ACL to interface to analyze and process the packets passing through this interface according to the MAC ACL.

Table 23 Configuring Application of MAC ACL to Interface

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure to apply MAC ACL to interface	<b>mac access-group</b> { <i>access-list-number</i>   <i>access-list-name</i> } { <b>in</b>   <b>out</b> }	Mandatory  By default, no MAC ACL is applied to interface.

### Note

- If the ACL applied to interface doesn't exist, all the packets passing through this interface will be permitted.

### Configure Application of HYBRID ACL to interface

Apply HYBRID ACL to interface to analyze and process the packets passing through this interface according to the HYBRID ACL.

Table 24 Configure Application of HYBRID ACL to Interface

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure to apply HYBRID ACL to interface	<b>hybrid access-group</b> { <i>access-list-number</i>   <i>access-list-name</i> } { <b>in</b>   <b>out</b> }	Mandatory  By default, no HYBRID ACL is applied to interface.

### Note

- If the ACL applied to interface doesn't exist, all the packets passing through this interface will be permitted.

### Configure Application of IPv6 ACL to Interface

Apply IPv6 ACL to interface to analyze and process the packets passing through this interface according to the IPv6 ACL.

Table 25 Configuring Application of IPv6 ACL to Interface

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure to apply IPv6 ACL to interface	<b>ipv6 access-group</b> { <i>access-list-number</i>   <i>access-list-name</i> } { <b>in</b>   <b>out</b> }	Mandatory  By default, no IPv6 ACL is applied to the interface.

---

 **Note**

- If the ACL applied to interface doesn't exist, all the packets passing through this interface will be permitted.
- 

### 95.2.12 Configure ACL mode

When the same ACL is applied on different ports, there are two modes. The first one is Port mode. In this mode, the same ACL uses different ACL resources on different ports, and the traffic on different ports uses different resources for matching. The other one is BitMap mode. In this mode, the same ACL uses the same ACL resources on different ports. Port matches through bitmaps. The traffic of different ports uses related resources for matching. Therefore, this mode can save resources. By default, the ACL is in Port mode.

#### Configuration Condition

None

#### Configure ACL mode

When the same ACL is used on different ports, mode can be utilized to adjust whether ACL will separately issues resources on the port or share resources through BitMap.

Table 26 Configuring ACL Mode

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure ACL mode	<b>acl mode { port   bitmap }</b>	Mandatory By default, ACL is in Port mode.

### 95.2.13 ACL Monitoring and Maintaining

Table 27 ACL Monitoring and Maintaining

Command	Description
<b>show access-list</b> [ <i>access-list-number</i>   <i>access-list-name</i> ]	Show the ACL configuration information
<b>show acl-object</b> [ <i>global</i>   <i>interface</i> [ <i>vlan</i> [ <i>in</i>   <i>out</i> ] ]   <i>switchport</i> [ <i>in</i>   <i>out</i>   <i>vfp</i> ] ]	Show the information of VLAN, port, global application of ACL, interface

Command	Description
<b>  vlan [ in   out ]   vlan-range [ in   out ] ]</b>	VLAN, VLAN RANGE, and interface VLAN RANGE
<b>show hybrid access-list</b> [ <i>access-list-number</i>   <i>access-list-name</i> ]	Show the configuration information of Hybrid extension and advanced ACL
<b>show ip access-list</b> [ <i>access-list-number</i>   <i>access-list-name</i> ]	Show the IP ACL configuration information
<b>show ip interface list</b>	Show the information of IP ACL applied to interface
<b>show ipv6 access-list</b> [ <i>access-list-number</i>   <i>access-list-name</i> ]	Show the configuration information of IPv6 ACL
<b>show mac access-list</b> [ <i>access-list-number</i>   <i>access-list-name</i> ]	Show the MAC ACL configuration information
<b>show mac interface list</b>	Show the information of MAC ACL applied to interface
<b>show time-range</b> [ <i>time-range-name</i> ]	Show the configuration of time domain and status information
<b>show time-range-state</b> [ <i>time-range-name</i> ]	Show status information of time domain
<b>show acl mode</b>	Show the information of ACL mode

## 95.3 Typical Configuration Example of ACL

### 95.3.1 Configure Standard IP ACL

#### Network Requirements

- PC1, PC2 and PC3 access IP network through the Device.
- Configure standard IP ACL rules so that PC1 instead of PC2 and PC3 can access the IP Network.

#### Network Topology

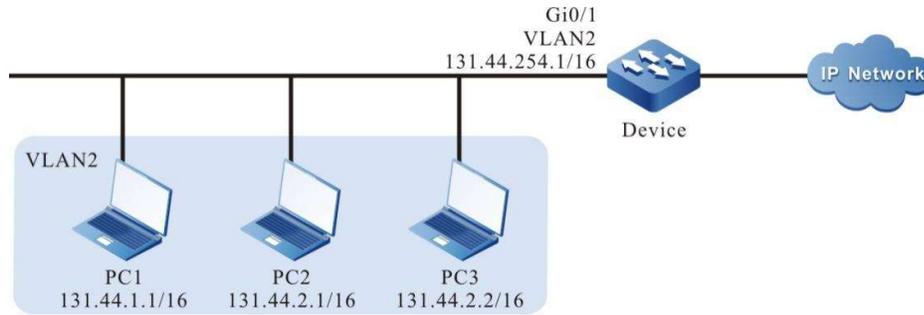


Figure 95 Network Topology for Configuring Standard IP ACL

## Configuration Steps

Step 1: Configure VLAN and port link type on Device.

#Create VLAN 2.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the link type of port gigabitethernet0/1 as Access to allow services of VLAN 2 to pass.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode access
Device(config-if-gigabitethernet0/1)#switchport access vlan 2
Device(config-if-gigabitethernet0/1)#exit
```

Step 2: Configure corresponding VLAN interface and IP address on the Device. (Omitted)

Step 3: Configure the standard IP ACL.

#Configure the standard IP ACL numbered 1 on Device.

```
Device(config)#ip access-list standard 1
```

#Configure rules to permit PC1 to access the IP Network.

```
Device(config-std-nacl)#permit host 131.44.1.1
```

#Configure rules to prevent the network segment 131.44.2.0/24 from accessing the IP Network.

```
Device(config-std-nacl)#deny 131.44.2.0 0.0.0.255
```

#Commit the rules configured

```
Device(config-std-nacl)#commit
Device(config-std-nacl)#exit
```

#View the information of ACL 1 on the Device.

```
Device#show ip access-list 1
ip access-list standard 1
10 permit host 131.44.1.1
20 deny 131.44.2.0 0.0.0.255
```

Step 4: Configure applying of the standard IP ACL.

#Apply the standard IP ACL numbered 1 to the ingress direction of port gigabitethernet0/1 of Device.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#ip access-group 1 in
Device(config-if-gigabitethernet0/1)#exit
```

#View on Device, the information of the ACL applied to the port.

```
Device#show acl-object interface
-----Interface-----Bind-----Instance-----
Interface-----Direction---AclType---AclName
gi0/1           IN      IP      1
-----Interface-----Bind-----Instance-----
Interface VlanId-----Direction---AclType---AclName
Device#
```

Step 5: Check the result.

#PC1 instead of PC2 and PC3 can access the IP Network.

### 95.3.2 Configure Extended IP ACL with Time Domain

#### Network Requirements

- PC1, PC2 and PC3 access IP network through the Device.
- Configure extended IP ACL rules so that PC1 can access the IP Network within the specified time, PC2 can access the FTP services in the IP Network, and PC3 cannot access the IP Network.

#### Network Topology

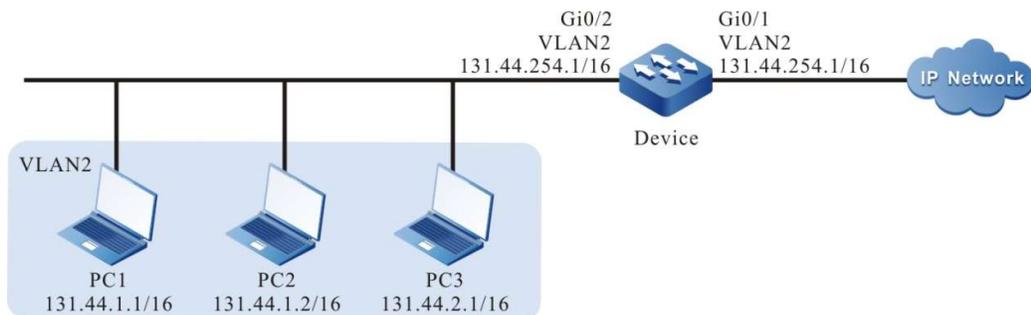


Figure 95 Network Topology for Configuring Extended IP ACL with Time Domain

#### Configuration Steps

Step 1: Configure VLAN and port link type on Device.

#Create VLAN 2.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the link type of the ports gigabitethernet0/1 and gigabitethernet0/2 as Access, permitting the services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/1,0/2
Device(config-if-range)#switchport mode access
Device(config-if-range)#switchport access vlan 2
Device(config-if-range)#exit
```

Step 2: Configure corresponding VLAN interface and IP address on the Device. (Omitted)

Step 3: Configure time domain.

#Configure time domain "time-range-work" on the Device, from 08:00:00 to 18:00:00 per day.

```
Device(config)#time-range time-range-work
Device(config-time-range)#periodic daily 08:00:00 to 18:00:00
Device(config-time-range)#exit
```

#View current system time on the Device.

```
Device#show clock

UTC FRI APR 05 15:26:31 2013
```

#View the information of defined time domain "time-range-work" on the Device.

```
Device#show time-range time-range-work
Timerange name:time-range-work (STATE:active)
10 periodic daily 08:00:00 to 18:00:00 (active)
```

Step 4: Configure extended IP ACL.

#Configure the extended IP ACL numbered 1001 on the Device.

```
Device(config)#ip access-list extended 1001
```

#Configure rules to prevent the network segment 131.44.2.0/24 from accessing the IP Network.

```
Device(config-ext-nacl)#deny ip 131.44.2.0 0.0.0.255 any
```

#Configure rules to permit PC2 to access the FTP services of IP Network.

```
Device(config-ext-nacl)#permit tcp host 131.44.1.2 any eq ftp
Device(config-ext-nacl)#permit tcp host 131.44.1.2 any eq ftp-data
```

#Configure rules to permit PC1 to access the IP Network within the scope of the defined time domain "time-range-work".

```
Device(config-ext-nacl)#permit ip host 131.44.1.1 any time-range time-range-work
```

#Commit the rules configured

```
Device(config-ext-nacl)#commit
Device(config-ext-nacl)#exit
```

#View the information of ACL 1001 on the Device.

```
Device#show ip access-list 1001
ip access-list extended 1001
10 deny ip 131.44.2.0 0.0.0.255 any
20 permit tcp host 131.44.1.2 any eq ftp
30 permit tcp host 131.44.1.2 any eq ftp-data
40 permit ip host 131.44.1.1 any time-range time-range-work (active)
```

Step 5: Configure to apply extended IP ACL.

#Apply the extended IP ACL numbered 1001 in the outgoing direction of port gigabitethernet0/1 of the Device.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#ip access-group 1001 out
Device(config-if-gigabitethernet0/1)#exit
```

#View on Device, the information of the ACL applied to the port.

```
Device#show acl-object interface
-----Interface-----Bind-----Instance-----
Interface-----Direction----AclType----AclName
gi0/1          OUT      IP      1001
-----Interface-----Bind-----Instance-----
Interface VlanId-----Direction----AclType----AclName
```

Step 6: Check the result.

#PC1 can access the IP Network from 08:00 to 18:00 per day; PC2 can access the FTP server in the IP Network, and PC3 cannot access the IP Network.

### 95.3.3 Configure Standard MAC ACL

#### Network Requirements

- PC1, PC2 and PC3 access IP network through the Device.
- Configure standard MAC ACL rules so that PC1 instead of PC2 and PC3 can access the IP Network.

#### Network Topology

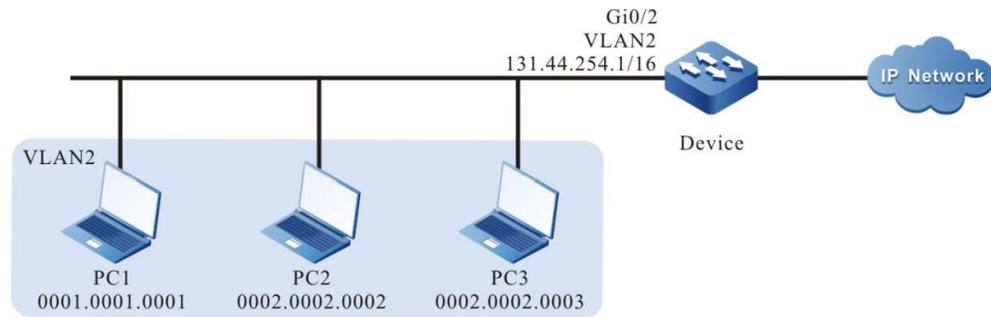


Figure 95 Network Topology for Configuring Standard MAC ACL

## Configuration Steps

Step 1: Configure VLAN and port link type on Device.

#Create VLAN 2.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the link type of port gigabitethernet0/2 to Access to allow services of VLAN 2 to pass.

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode access
Device(config-if-gigabitethernet0/2)#switchport access vlan 2
Device(config-if-gigabitethernet0/2)#exit
```

Step 2: Configure corresponding VLAN interface and IP address on the Device. (Omitted)

Step 3: Configure standard MAC ACL.

#Configure the standard MAC ACL numbered 2001 on the Device.

```
Device(config)#mac access-list standard 2001
```

#Configure rules to permit PC1 to access the IP Network.

```
Device(config-std-mac-nacl)#permit host 0001.0001.0001
```

#Configure rules to prevent the network segment with MAC address of 0002.0002.0000 and mask of ffff.ffff.0000 from accessing the IP Network.

```
Device(config-std-mac-nacl)#deny 0002.0002.0000 0000.0000.ffff
```

#Commit the rules configured

```
Device(config-std-mac-nacl)#commit
```

#View the information of ACL 2001 on the Device.

```
Device#show mac access-list 2001
mac access-list standard 2001
10 permit host 0001.0001.0001
20 deny 0002.0002.0000 0000.0000.ffff
```

Step 4: Configure to apply standard MAC ACL.

#Apply the standard MAC ACL numbered 2001 in the incoming direction of port gigabitethernet0/1 of the Device.

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#mac access-group 2001 in
Device(config-if-gigabitethernet0/2)#exit
```

#View on Device, the information of the ACL applied to the port.

```
Device#show acl-object interface
-----Interface----Bind----Instance-----
Interface-----Direction---AclType---AclName
gi0/2           IN      MAC     2001
-----Interface----Bind----Instance-----
Interface VlanId-----Direction---AclType---AclName
```

Step 5: Check the result.

#PC1 instead of PC2 and PC3 can access the IP Network.

### 95.3.4 Configure Extended MAC ACL

#### Network Requirements

- PC1, PC2 and IP Phone access the IP network through Device1.
- Configure extended MAC ACL rules on Device2 so that VLAN2 users cannot access the IP Network, and VLAN3 users others than voice users can access it.

#### Network Topology

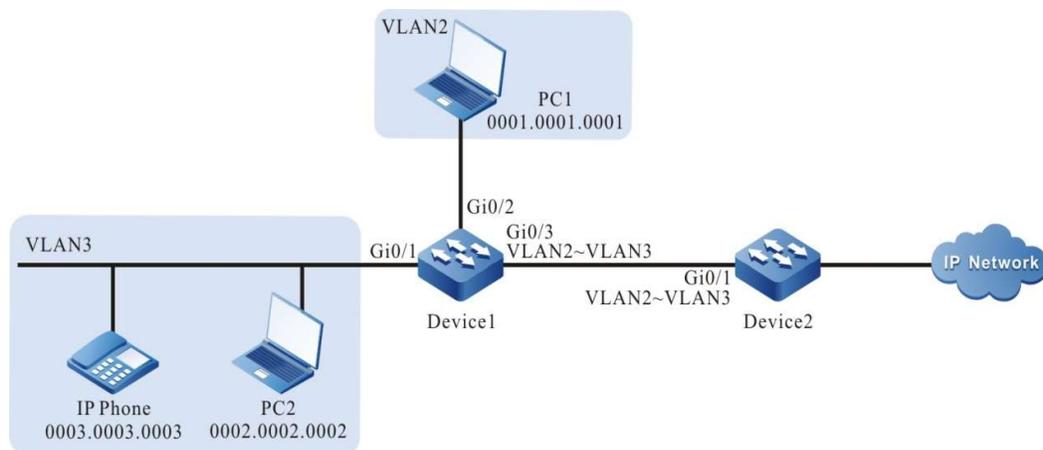


Figure 95 Network Topology for Configuring Extended MAC ACL

### Configuration Steps

Step 1: Configure VLAN and port link type on Device2.

#Create VLAN2 and VLAN3.

```
Device2#configure terminal
Device2(config)#vlan 2
Device2(config-vlan2)#exit
```

```
Device2#configure terminal
Device2(config)#vlan 3
Device2(config-vlan3)#exit
```

#Configure the link type of port gigabitethernet0/1 as Trunk, and allow services of VLAN2 and VLAN3 to pass.

```
Device2(config)#interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#switchport mode trunk
Device2(config-if-gigabitethernet0/1)#switchport trunk vlan 2-3
Device2(config-if-gigabitethernet0/1)#exit
```

Step 2: Configure corresponding VLAN interface and IP address on Device1 and Device2. (Omitted)

Step 3: Configure Voice-VLAN on Device1 and set the cos value of IP Phone packet as 7. (omitted)

Step 4: Configure extended MAC ACL.

#Configure the extended MAC ACL numbered 3001 on Device2.

```
Device2(config)#mac access-list extended 3001
```

#Configure rules to prevent the users in VLAN2 from accessing the IP Network.

```
Device2(config-ext-mac-nacl)#deny any any vlan-id 2
```

#Configure rules to prevent the voice users in VLAN3 from accessing the IP Network.

```
Device2(config-ext-mac-nacl)#deny any any cos 7 vlan-id 3
```

#Configure rules to prevent other users in VLAN3 from accessing the IP Network.

```
Device2(config-ext-mac-nacl)#permit any any vlan-id 3
```

#Commit the rules configured

```
Device2(config-ext-mac-nacl)#commit
```

#View the information of ACL 3001 on Device2.

```
Device2#show access-list 3001
mac access-list extended 3001
10 deny any any vlan-id 2
20 deny any any cos 7 vlan-id 3
30 permit any any vlan-id 3
```

Step 5: Configure to apply extended MAC ACL.

#Apply the extended MAC ACL numbered 3001 in the incoming direction of port gigabitethernet0/1 of Device2.

```
Device2(config)#interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#mac access-group 3001 in
Device2(config-if-gigabitethernet0/1)#exit
```

#View on Device2 the information of the ACL applied to the port.

```
Device#show acl-object interface
-----Interface----Bind----Instance-----
Interface-----Direction----AclType----AclName
gi0/1           IN      MAC      3001
-----Interface----Bind----Instance-----
Interface VlanId-----Direction----AclType----AclName
```

Step 6: Check the result.

#PC2 instead of PC1 and IP Phone can access the IP Network.

---

### Note

- For configurations related to Voice-VLAN, refer to the Voice-VLAN-related chapter in the User Manual.
- 

## 95.3.5 Configure Extended Hybrid ACL

### Network Requirements

- PC1, PC2 and PC3 access IP network through the Device.
- Configure extended Hybrid ACL rules so that PC1 instead of PC2 and PC3 can access the

IP Network within the specified time range.

## Network Topology

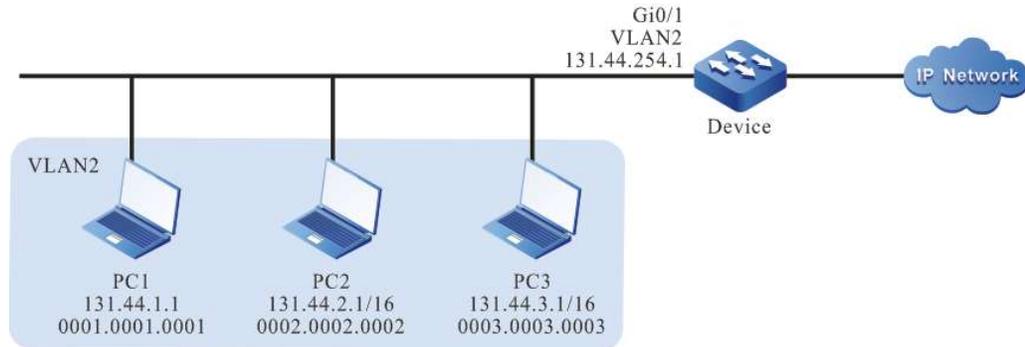


Figure 95 Network Topology for Configuring Extended Hybrid ACL

## Configuration Steps

Step 1: Configure VLAN and port link type on Device.

#Create VLAN 2.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the link type of port gigabitethernet0/1 as Access to allow services of VLAN 2 to pass.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode access
Device(config-if-gigabitethernet0/1)#switchport access vlan 2
Device(config-if-gigabitethernet0/1)#exit
```

Step 2: Configure corresponding VLAN interface and IP address on the Device. (Omitted)

Step 3: Configure time domain.

#Configure time domain "time-range-work" on the Device, from 08:00 to 18:00 per day.

```
Device(config)#time-range time-range-work
Device(config-time-range)#periodic daily 08:00 to 18:00
Device(config-time-range)#exit
```

#View current system time on the Device.

```
Device#show clock
UTC FRI APR 05 15:26:31 2013
```

#View the information of defined time domain "time-range-work" on the Device.

```
Device#show time-range time-range-work
Timerange name:time-range-work (STATE:active)
10 periodic daily 08:00 to 18:00 (active)
```

Step 4: Configure extended Hybrid ACL.

#Configure the extended Hybrid ACL numbered 5001 on the Device.

```
Device(config)#hybrid access-list extended 5001
```

#Configure rules to permit PC1 to access the IP Network within the scope of the defined time domain "time-range-work".

```
Device(config-hybrid-nacl)# permit host 0001.0001.0001 any ether-type ipv4 ip any any time-range time-range-workwork
```

#Configure rules to prevent the network segment 131.44.0.0/16 from accessing the IP Network.

```
Device(config-hybrid-nacl)# deny any any ether-type ipv4 ip 131.44.0.0 0.0.255.255 any
```

#Configure rules to permit all the packets from IP Network to pass through the Device.

```
Device(config-hybrid-nacl)# permit any any ether-type ipv4 ip any any
```

#Commit the rules configured

```
Device(config-hybrid-nacl)#commit  
Device(config-hybrid-nacl)#exit
```

#View the information of ACL 5001 on the Device.

```
Device#show hybrid access-list 5001  
hybrid access-list extended 5001  
  
10 permit host 0001.0001.0001 any ether-type ipv4 ip any any time-range time-range-work (active)  
20 deny any any ether-type ipv4 ip 131.44.0.0 0.0.255.255 any  
30 permit any any ether-type ipv4 ip any any
```

Step 5: Configure to apply extended Hybrid ACL.

#Apply the extended Hybrid ACL numbered 5001 in the incoming direction of global.

```
Device(config)#global hybrid access-group 5001 in
```

#View on Device the information of the ACL applied globally.

```
Device#show acl-object global  
  
-----Global----Bind----Instance-----  
Global-----Direction----AclType----AclName  
global          IN      HYBRID    5001
```

Step 6: Check the result.

#PC1 can access the IP Network from 08:00 to 18:00 per day; PC2 and PC3 cannot access the IP Network.

# 96 Attack Detection

## 96.1 Overview

Attack defense is an important function for the maintenance of network security. It analyzes the content of packets passing through the device to determine whether they have the characteristics of attack, and takes some preventive measures for those with attack characteristics according to the configuration, such as intercepting attack packet, recording attack packet log, and adding attack source to blacklist. By configuring the device with attack defense function, on one hand, you can prevent the device from becoming abnormal due to network attack to improve the device's anti-attack ability; on the other hand, the attack traffic forwarded by the device can be intercepted to prevent other devices on the network from working abnormally due to the attack.

## 96.2 Attack Defense Function Configuration

Table 96 Attack Defense Function Configuration List

Configuration Task	
Configure single-packet attack defense function	<p>1) Hardware detection supports the configuration of intercepting the following attack packets: frag-icmp, icmp-large, icmpv6-large, ping-of-death, smurf, src-dst-mac-equal, src-dst-ip-equal, src-dst-port-equal, tcp-flag-seq-zero, tcp-hdr-incomplete, tcp-invalid-flag, tcp-syn-fin, smac-zero, and invalid-ttl. The actual results are subject to the capability set of each chip.</p> <p>2) Configure to intercept the following attack packets for software: fraggle, fragment, tcp-land, REDIRECT, UNREACH, ECHOREPLY, SOURCEQUENCH, ECHO, ROUTERADVERT, ROUTERSOLICIT, TIMXCEED, PARAMPROB, TSTAMP, TSTAMPREPLY, IREQ, IREQREPLY, MASKREQ, MASKREPLY, small-packet, and icmp code none-zero.</p>
Configure flood defense function	Configure to intercept the following types of flood attack packets: tcp syn, tcp syn-ack, tcp

	ack, tcp fin, tcp rst, tcp port, udp, udp port, icmp, icmpv6, dns, http, and ip.
Configure scanning attack defense function	Configure to intercept ip scanning and port scanning attack packets
Configure URPF attack defense function	Configure URPF check function
Configure blacklist function	Configure blacklist function and discard the packets of corresponding source address

Note: The packet interception configured on software of the switch is applicable to the packet of local device only.

### 96.2.1 Configure Single-packet Attack Defense Function

Single-packet attack defense can determine whether the packets passing through the device are offensive by analyzing their characteristics. Generally, it is only valid for the packets applied with attack defense policies in the incoming direction. After the single-packet attack defense function is configured, if the device finds that a packet is offensive, it will output an alarm log, discard the packet, and perform statistics of discarded packets.

#### Configuration Condition

None

#### Configure Different Types of Single-packet Attack Defense Function

When the attack packet configured is detected, it will be discarded, and statistics of discarded packets will be performed.

Table 96 Configuring Single-packet Attack List

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure to intercept specified type of single-packet attack packet	<b>anti-attack detect { fraggle   frag-icmp   icmp-large   icmpv6-large   ping-of-death   src-dst-ip-equal   src-dst-mac-equal   src-dst-port-equal   smurf   tcp-flag-seq-zero   tcp-hdr-incomplete   tcp-invalid-</b>	Mandatory By default, the default value of <i>max-off</i> is 65535.

	<b>flags   tcp-land   tcp-syn-fin   smac-zero   invalid-ttl}</b>  <b>anti-attack drop { fragment [ max-off max-off ]   small-packet [ mini-length ]   icmp { type { REDIRECT   UNREACH   ECHOREPLY   SOURCEQUENCH   ECHO   ROUTERADVERT   ROUTERSOLICIT   TIMXCEED   PARAMPROB   TSTAMP   TSTAMPREPLY   IREQ   IREQREPLY   MASKREQ   MASKREPLY}   code none-zero }}</b>  <b>anti-attack subnet-broadcast masklen length</b>	By default, the default value of <i>mini-length</i> is 64.  By default, the default value of <i>length</i> is 0.  For single-packet attack defense, the detection of packets with such characteristics is disabled.
--	---	---

### Configure Single-packet Attack Defense Logging

When the device finds single-packet attack, it discards the packet while logging.

Table 96 Configuring Single-packet Attack Log Output

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure single-packet attack type of log output	<b>attack-defense action logging detect</b>	Mandatory  By default, the single-packet attack defense log is not enabled.

## 96.2.2 Configure Flood Defense Function

Flood attack is mainly used to protect servers from the impact of large-traffic packets. Generally, it is applied to the interface of the device connecting external network, and valid for the packets in the incoming direction of the interface where the attack defense policy is applied. After the flood defense policy is applied to the interface, the interface begins to detect attack. When it finds that the rate of a certain type of keeps exceeding the specified trigger threshold value, it considers that the interface has been flooded and enters the attack defense status. Then, it starts corresponding defense policy according to the configuration (output alarm logs, discard packets, and add attack source to the dynamic blacklist which takes effect after traceability function is configured). When the device finds the traffic of this type of

packet is less than the threshold value for 5 seconds in succession, the attack status is cancelled, and attack defense measures stop.

### Configuration Condition

Configure attack defense policy, and flood defense in the policy configuration mode.

Apply attack defense policy, and enable the flood defense detection in the policy.

### Configure Different Types of Flood Defense Function

When the packet configured with flood detection exceeds the threshold value, corresponding defense measures should be taken.

Table 96 Configuring Flood Defense List

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the policy configuration mode	<b>attack-defense policy <i>policy</i></b>	Mandatory The defense policy is differentiated according to policy name
Configure flood detection type and defense action	<b>detect { tcp-syn   tcp-ack   tcp-syn-ack   tcp-fin   tcp-rst   tcp { port [ <i>port-number</i>   bgp   ftp   ldp   ssh   syslog   telnet ] }   udp { port [ <i>port-number</i>   snmp   syslog   tftp ] }   icmp   icmpv6   dns   http   ip } flood threshold <i>threshold-value</i> action { drop   blacklist }*</b>	<b>threshold-value:</b> Configure the threshold value of flood detection  By default, corresponding type of flood detection is not enabled.  When the policy is applied, corresponding flood detection function takes effect.

### Configure the Function of Tracing Attack Source in Flood Detection

Trace the packet configured with flood defense, and summarize the number of packets based on each source address.

Table 96 Configuring Flood Defense and Tracing Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the policy configuration mode	<b>attack-defense policy <i>policy</i></b>	Mandatory The defense policy is differentiated according to policy name
Configure flood defense and tracing function	<b>trace-type {source-ip   source-mac} max-count <i>max-source-number</i></b>	<i>max-source-number</i> : Configure the number of packets for flood detection and tracing. For the node of the source address where tracing number is exceeded, tracing operation is not performed.  By default, the detection of unisource threshold value is not performed according to the source address.

**Configure Global Application of Attack Defense Policy**

Flood attack is configured based on policy, and the configuration takes effect when the policy is applied.

Table 96 Configuring Global Application of Flood Defense Policy

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Configure application of attack defense policy	<b>attack-defense global apply policy</b> <i>policy-name</i>	By default, all flood defense functions are invalid.  <i>policy-name</i> : Enable specific defense policy
--	---	---

### Configure Application of Attack Defense Policy Under the Port

Flood attack is configured based on policy, and the configuration takes effect when the policy is applied. The policy can be separately applied based on interface. If there is both global application policy and configuration under interface, the latter takes valid first.

Table 96 Configure Application of Attack Defense Policy Under Interface

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the L2/L3 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  The subsequent configuration takes effect only on the current interface after you enter the L2/L3 Ethernet interface configuration mode
Configure application of attack defense policy	<b>attack-defense apply policy</b> <i>policy-name</i>	By default, the policy is not separately applied under interface.  <i>policy-name</i> : Enable specific defense policy

### Configure Flood Defense Logging

When the device finds flood attack, it takes defense policies while logging.

Table 96 Configuring Flood Attack Log Output

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure flood attack log output	<b>attack-defense action logging flood</b>	By default, the flood defense log is not enabled.

### 96.2.3 Configure Scanning Attack Defense Function

Scanning attack defense mainly detects the detection behavior by monitoring the rate of initiating connections to the target system by network users to prevent them from detecting network status. Generally, it is applied to the interface of the device connecting external network, and valid for the packets in the incoming direction of the interface where the attack defense policy is applied.

After the scanning attack defense is configured, when the number of IPs accessed in the network or the number of ports accessed on a certain device exceeds the threshold value, it is considered that a scanning attack has happened in the network, and the attack source is automatically detected and added to the dynamic blacklist. At the same time, a scanning attack defense log will be output according to the configuration.

#### Configuration Condition

Configure attack defense policy, and scanning attack defense in the policy configuration mode.

Apply attack defense policy, and enable the scanning attack defense detection in the policy.

#### Configure Scanning Attack Defense Function

After the scanning attack defense level is configured, and the number of destination addresses accessed in the network or the number of ports accessed on a certain destination address exceeds the threshold value, a scanning attack log will be output according to the configuration and the attack source will be added to the blacklist.

High means high-level defense. The number of destination IP addresses permitted for simultaneous access at this level is 16, and 4 ports are permitted for simultaneous access under the same destination address. Medium means medium-level defense. This level allows 32 destination IP addresses to be accessed at the same time and 8 ports to be accessed simultaneously under the same destination address. Low means low-level defense. The number of destination IP addresses permitted for simultaneous access at this level is 64, and 16 ports can be accessed simultaneously under the same destination address.

Table 96 Configure Scanning Attack Defense Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the policy configuration mode	<b>attack-defense policy <i>policy</i></b>	Mandatory The defense policy is differentiated according to policy name
Configure scanning attack defense function	<b>detect scan level {high   medium   low} action blacklist</b>	By default, the scanning attack defense function is not enabled.  When the policy is applied, corresponding scanning attack detection function takes effect.

### Configure Global Application of Attack Defense Policy

Scanning attack is configured based on policy, and the configuration takes effect when the policy is applied.

Table 1 Configuring Global Application of Attack Defense Policy

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure application of attack defense policy	<b>attack-defense global apply policy <i>policy-name</i></b>	By default, the scanning attack defense function is invalid.  <i>policy-name</i> : Enable specific defense policy

### Configure Application of Attack Defense Policy Under the Port

Scanning attack is configured based on policy, and the configuration takes effect when the policy is applied. The policy can be separately applied based on interface. If there is both global application policy and configuration under interface, the latter takes valid first.

Table 2 Configure Application of Attack Defense Policy Under Interface

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the L2/L3 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  The subsequent configuration takes effect only on the current interface after you enter the L2/L3 Ethernet interface configuration mode
Configure application of attack defense policy	<b>attack-defense apply policy</b> <i>policy-name</i>	By default, the policy is not separately applied under interface.  <i>policy-name</i> : Enable specific defense policy

### Configure Scanning Attack Defense Logging

When the device finds any scanning attack, it begins logging.

Table 96 Configuring Scanning Attack Log Output

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure scanning	<b>attack-defense action logging scan</b>	By default, the scanning attack

attack log output		defense log is not enabled.
-------------------	--	-----------------------------

## 96.2.4 Configure URPF Attack Defense Function

URPF, a unicast reverse routing lookup technology, is used to prevent the attacks based on source address spoofing, such as DoS (Denial of Service) and DDoS (Distributed Denial of Service) attacks.

### Configuration Condition

To make the URPF detection take effect, you are required to globally enable the URPF function.

### Configure Global URPF Function

The URPF function on the interface takes effect only after the URPF function is globally enabled.

Table 3 Configuring Global URPF Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure global URPF function	<b>ip urpf</b>	Mandatory Enable the global URPF function

### Configure the Function of Looking up Default Route via URPF

When looking up the source route via URPF, permit the packet to pass if its source route is found to be the default route by enabling the default route function. Table 4 Configuring Permission of Default Route via URPF

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Configure permission of default route via URPF	<b>ip urpf allow-default-route</b>	Enable permission of default route via URPF  It is not enabled by default.
--	------------------------------------	--

### 。 Configure URPF Function Under Interface

When looking up the source route via URPF, permit the packet to pass if its source route is found to be the default route by enabling the default route function.

In the loose mode, only whether the source address is in the routing table will be checked; in the strict mode, whether the source address is in the routing table and whether the incoming port of the packet is correct will be checked.

Table 96 Configuring Permission of Default Route via URPF

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	<i>interface-name</i> : Configure the interface of URPF function
Configure the URPF detection function on interface	<b>ip urpf { loose   strict }</b>	Enable the URPF detection function on interface. The URPF function is not enabled by default.

## 96.2.5 Configure Blacklist Function

The blacklist function is an attack defense feature which filters packets according to the source IP or IPv6 address of packets. Compared to the packet filtering function based on ACL (Access Control List), blacklist uses a simple way to match packets. It can rapidly filter and effectively shield packets. Blacklist can be added or deleted by the device dynamically or the user manually.

### Configuration Condition

None

## Configure Static Blacklist

Dynamic blacklist is dynamically added by functions like flood defense and scanning attack defense, while static blacklist is manually configured by the user.

The blacklist on the switching device is implemented through ACL resources, and that on the routing device is implemented through software.

Table 5 Configuring Static Blacklist

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure static blacklist	<b>blacklist {ip <i>ip-address</i>   ipv6 <i>ipv6-address</i> }</b>	<i>ip-address</i> and <i>ipv6-address</i> are used to configure the blacklist function of specified source address.

## 96.2.6 Attack Defense Monitoring and Maintaining

Table 6 Attack Defense Monitoring and Maintaining List

Step	Command	Description
Clear statistics of NULL SCAN on all members	<b>clear attack-defense nullscan stastics</b>	-
Show statistics of single-packet attack	<b>show anti-attack detect statistic lpu <i>lpu-ID</i></b>	-
Show the attack defense policy	<b>show attack-defense applied policy</b>	-

applied at present		
Show the configuration of attack defense policy	<b>show attack-defense policy</b> [ <i>policy-name</i> ]	-
Show flood defense status	<b>show attack-defense flood lpu</b> <i>lpu-ID</i> [ <b>interface</b> <i>interface-name</i> ]	-
Show scanning attack defense status	<b>show attack-defense scan</b> { <b>ip-scan</b>   <b>ipv6-scan</b>   <b>port-scan</b>   <b>ipv6-port-scan</b> } <b>lpu</b> <i>lpu-ID</i>	-
Show the scanning attack defense status on the specified interface	<b>show attack-defense scan</b> { <b>statistic</b>   <b>ipv6-statistic</b> } <b>lpu</b> <i>lpu-ID</i> <b>interface</b> <i>interface-name</i>	-
Show attack tracing status	<b>show attack-defense trace lpu</b> <i>lpu-ID</i> [ <b>interface</b> <i>interface-name</i> ]	-
Show the information of blacklist	<b>show blacklist</b> { <b>ip</b>   <b>ipv6</b>   <b>config</b>   <b>mac</b> } <b>lpu</b> <i>lpu-ID</i>	-
Show the statistics of NULL SCAN	<b>show attack-defense nullscan stastics</b> <b>lpu</b> <i>lpu-ID</i>	When the flood defense function is enabled, the nullscan (the packet with the flag of 0 in TCP packet) detection function will be automatically enabled.

## 96.3 Typical Configuration Example of Attack Defense

### 96.3.1 Configure Single-packet Attack Detection

#### Network Requirements

- The attacker and PC access the Device through interface.
- The single-packet attack detection function is configured for the Device so that it can give an alarm when an attack packet is detected and discards it. Take common Fraggle and Land attacks as examples.

#### Network Topology

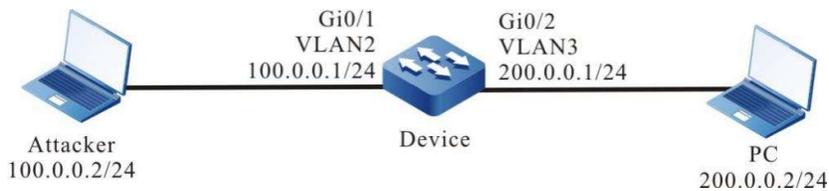


Figure 96 Network Topology for Configuring Single-packet Attack Detection

#### Configuration Steps

- Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)
- Step 2: Configure the IP address and route of each interface, and require PC to access the Network through the Device. (Omitted)
- Step 3: Configure Fraggle and Land attack detection function on the Device and turn on the single-packet attack log switch.

#Configure Fraggle attack detection.

```
Device#configure terminal
Device(config)#anti-attack detect fraggle
```

#Configure Land attack detection.

```
Device(config)#anti-attack detect top-land
```

#Turn on the single-packet attack log switch on the Device.

```
Device(config)#attack-defense action logging detect
```

- Step 4: Check the result.

#When the attacker launches Fraggle and Land attacks on the PC, if this function is not configured, the attack packets can be captured on the PC; if this function is configured, the attack packets cannot be captured on the PC, in which case, you need to check log and statistical information on the Device.

#When there is a Fraggle attack on the Device, it will output the following log information:

```
%ANTIATTACK-DETECT_ATTACK-4: vlan2 detect attack, type fraggle
```

#When there is a Land attack on the Device, it will output the following log information:

```
%ANTIATTACK-DETECT_ATTACK-4: vlan2 detect attack, type tcp-land
```

#Execute the command show anti-attack detect statistic on the Device to view the statistical information of discarded packets.

```
Device#show anti-attack detect statistic
```

detect-type	DropCount
-----	
fraggle	87
fragment	0
frag-icmp	0
tcp-land	456
REDIRECT	0
UNREACH	0
ECHOREPLY	0
SOURCEQUENCH	0
ECHO	0
ROUTERADVERT	0
ROUTERSOLICIT	0
TIMXCEED	0
PARAMPROB	0
TSTAMP	0
TSTAMPREPLY	0
IREQ	0
IREQREPLY	0
MASKREQ	0
MASKREPLY	0
small-packet	0
none-zero	0
invalid-ttl	0

---

### Note

- The hardware processing of single-packet attack detection on the switch is valid for both forwarded and local packets, and no log or statistical information will be generated; the software processing of single-packet attack detection is only valid for local packets, and log and statistical information will be generated.
-

## 96.3.2 Configure Flood Attack Detection

### Network Requirements

- The Device accesses the IP Network through gigabitethernet0/1.
- The flood attack detection function is configured for the Device so that it can give an alarm log when an attack packet of corresponding type is detected and discards it. Take common tcp syn flood and icmp flood attacks as examples.

### Network Topology

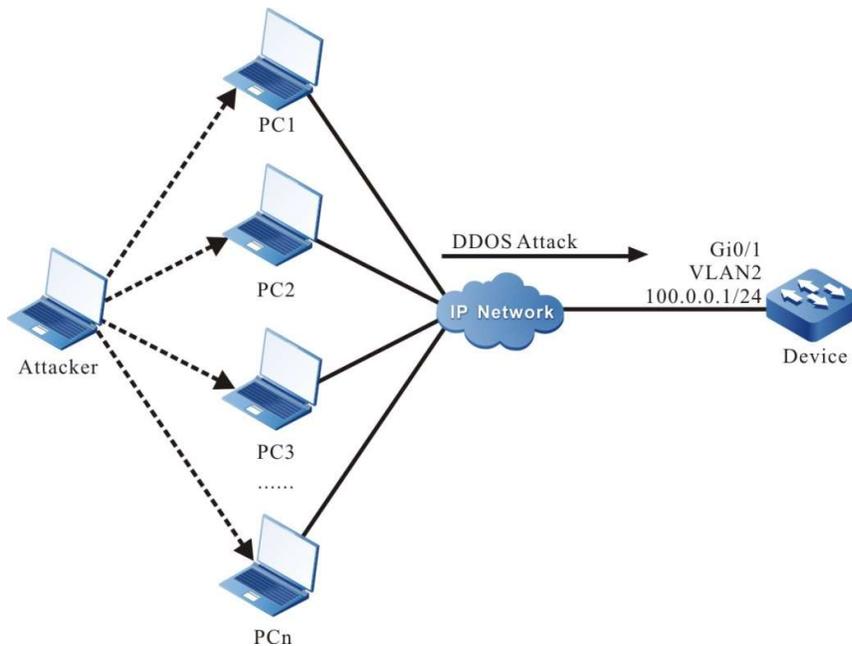


Figure 96 Network Topology for Configuring Flood Attack Detection

### Configuration Steps

- Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)
- Step 2: Configure the IP address and route of each interface, and require PC to access the IP Network through the Device. (Omitted)
- Step 3: Configure attack defense policy a on the Device, add tcp syn flood and icmp flood attack detection function to the policy, and configure IP address-based attack traceability.

```
Device(config)#attack-defense policy a
Device(config-anti-policy-a)#detect tcp-syn flood threshold 500 action drop
Device(config-anti-policy-a)#detect icmp flood threshold 500 action blacklist
Device(config-anti-policy-a)#trace-type source-ip max-count 5
Device(config-anti-policy-a)#exit
```

#Configure global application of attack defense policy a on the Device.

```
Device(config)#attack-defense global apply policy a
```

#Turn on the flood attack log switch on the Device.

```
Device(config)#attack-defense action logging flood
```

Step 4: Check the result.

#View current attack defense policy on the Device.

```
Device#show attack-defense applied policy
attack-defense policy a
detect tcp-syn flood threshold 500 action drop
detect icmp flood threshold 500 action blacklist
trace-type source-ip max-count 5
```

#When an attacker launches tcp syn flood and icmp flood attacks on the Device, view the flood attack log output on the Device.

```
%ANTIATTACK-FLOOD_ATTACK-4: vlan2 detect attack, type tcp-syn.
%ANTIATTACK-FLOOD_IP_ATTACK-4: vlan2 detect attack, type icmp, ipaddr 100.0.0.2.
```

#View attack tracing entries on the Device.

```
Device#show attack-defense trace lpu 0
Trace Info:
IpAddr, Interface
Type      DropCount  Token      LastRecvTime
-----
100.0.0.2, vlan2
icmp      , 0        , 299      , Sun Apr 25 10:58:43 2021
tcp-syn   , 0        , 349      , Sun Apr 25 10:58:43 2021
100.0.0.5, vlan2
icmp      , 0        , 392      , Sun Apr 25 10:58:43 2021
tcp-syn   , 0        , 366      , Sun Apr 25 10:58:43 2021
100.0.0.4, vlan2
icmp      , 0        , 391      , Sun Apr 25 10:58:43 2021
tcp-syn   , 0        , 351      , Sun Apr 25 10:58:43 2021
100.0.0.3, vlan2
icmp      , 0        , 391      , Sun Apr 25 10:58:43 2021
tcp-syn   , 0        , 367      , Sun Apr 25 10:58:43 2021
100.0.0.2, gigabitethernet0/1
icmp      , 0        , 299      , Sun Apr 25 10:58:43 2021
tcp-syn   , 0        , 349      , Sun Apr 25 10:58:43 2021
100.0.0.5, gigabitethernet0/1
```

```

icmp      , 0      , 392      , Sun Apr 25 10:58:43 2021
tcp-syn   , 0      , 366      , Sun Apr 25 10:58:43 2021
100.0.0.4, gigabitethernet0/1
icmp      , 0      , 391      , Sun Apr 25 10:58:43 2021
tcp-syn   , 0      , 349      , Sun Apr 25 10:58:43 2021
100.0.0.3, gigabitethernet0/1
icmp      , 0      , 391      , Sun Apr 25 10:58:43 2021
tcp-syn   , 0      , 366      , Sun Apr 25 10:58:43 2021

```

#View flood attack defense status on the Device.

```

Device#show attack-defense flood lpu 0

Flood Info:

Type      DropCount  Token      LastRecvTime
-----
vlan2
icmp      , 0      , 217      , Sun Apr 25 10:58:49 2021
tcp-syn   , 5867    , 148      , Sun Apr 25 10:58:49 2021
gigabitethernet0/1
icmp      , 0      , 217      , Sun Apr 25 10:58:49 2021
tcp-syn   , 0      , 0        , Sun Apr 25 10:58:47 2021

```

#View the dynamic blacklist entries generated by tracing on the Device.

```

Device#show blacklist ip lpu 0

Blacklist Info:

IpAddr,      CreateTime,      Agetime
-----
100.0.0.2    , Sun Apr 25 10:58:50 2021 , 118

```

### 96.3.3 Configure Scanning Attack Detection

#### Network Requirements

- The Device accesses the IP Network through gigabitethernet0/1.
- Scanning attack detection function is configured on the Device. When IP scanning or Port scanning is detected, output an alarm log, add the attack source to the blacklist, and intercept all packets of the attack source before aging of the blacklist.

#### Network Topology

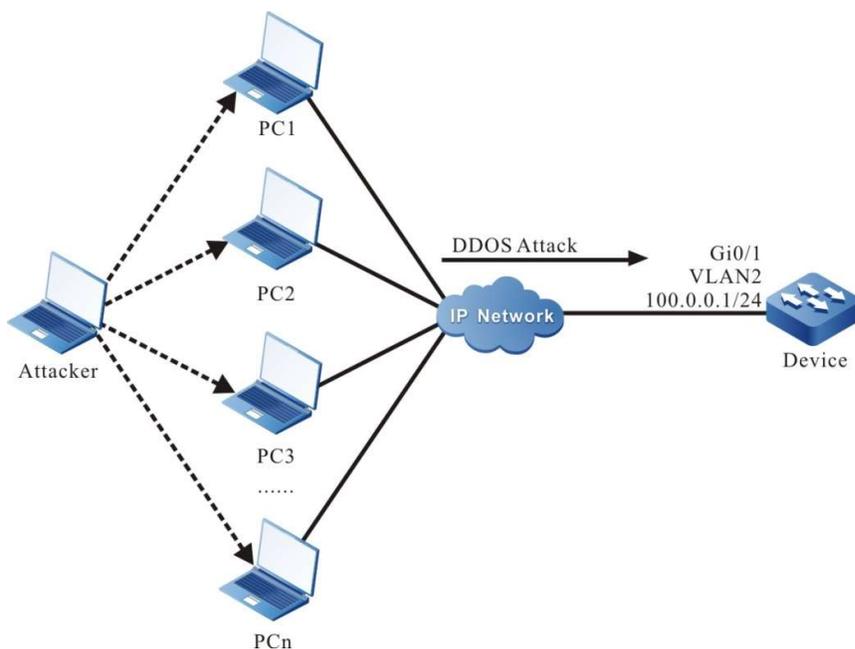


Figure 96 Network Topology for Configuring Scanning Attack Detection

### Configuration Steps

Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configure the IP address and route of each interface, and require PC to access the IP Network through the Device. (Omitted)

Step 3: Configure attack defense policy a on the Device, and the scanning attack detection function in the policy, with the scanning level being high.

```
Device(config)#attack-defense policy a
Device(config-anti-policy-a)#detect scan level high action blacklist
Device(config-anti-policy-a)#exit
```

#Configure global application of attack defense policy a on the Device.

```
Device(config)#attack-defense global apply policy a
```

#Turn on the scanning attack log switch on the Device.

```
Device(config)#attack-defense action logging scan
```

Step 4: Check the result.

#View current attack defense policy on the Device.

```
Device#show attack-defense applied policy
attack-defense policy a
detect scan level high action blacklist
```

#When an attacker launches a scanning attack on the Device, view the scanning attack log output on the Device.

```
%ANTIATTACK-SCAN_PORT_ATTACK-4: vlan2 detect port scan attack.  
%ANTIATTACK-SCAN_PORT_ATTACK-4:Detect 100.0.0.2 is attacking the system.  
%ANTIATTACK-SCAN_IP_ATTACK-4: vlan2 detect ip scan attack.
```

#View attack IP scanning entries on the Device.

```
Device#show attack-defense scan ip-scan lpu 0  
IP Scan Statistic :  
sip          dip-count    interface  
-----  
100.0.0.3    4            vlan2  
100.0.0.4    4            vlan2  
100.0.0.5    4            vlan2  
100.0.0.6    4            vlan2  
100.0.0.3    4            gigabitethernet0/1  
100.0.0.4    4            gigabitethernet0/1  
100.0.0.5    4            gigabitethernet0/1  
100.0.0.6    4            gigabitethernet0/1
```

#View Port scanning entries on the Device.

```
Device#show attack-defense scan port-scan lpu 0  
Port Scan Statistic :  
sip          dip          dport-count  interface  
-----  
100.0.0.3    101.0.0.1    1            vlan2  
100.0.0.3    101.0.0.2    1            vlan2  
100.0.0.3    101.0.0.3    1            vlan2  
100.0.0.3    101.0.0.4    1            vlan2  
100.0.0.4    101.0.0.5    1            vlan2  
100.0.0.4    101.0.0.6    1            vlan2  
100.0.0.4    101.0.0.7    1            vlan2  
100.0.0.4    101.0.0.8    1            vlan2  
100.0.0.5    101.0.0.9    1            vlan2  
100.0.0.5    101.0.0.10   1            vlan2  
100.0.0.5    101.0.0.11   1            vlan2  
100.0.0.5    101.0.0.12   1            vlan2  
100.0.0.6    101.0.0.13   1            vlan2  
100.0.0.6    101.0.0.14   1            vlan2
```

100.0.0.6	101.0.0.15	1	vlan2
100.0.0.6	101.0.0.16	1	vlan2
100.0.0.3	101.0.0.1	1	gigabitethernet0/1
100.0.0.3	101.0.0.2	1	gigabitethernet0/1
100.0.0.3	101.0.0.3	1	gigabitethernet0/1
100.0.0.3	101.0.0.4	1	gigabitethernet0/1
100.0.0.4	101.0.0.5	1	gigabitethernet0/1
100.0.0.4	101.0.0.6	1	gigabitethernet0/1
100.0.0.4	101.0.0.7	1	gigabitethernet0/1
100.0.0.4	101.0.0.8	1	gigabitethernet0/1
100.0.0.5	101.0.0.9	1	gigabitethernet0/1
100.0.0.5	101.0.0.10	1	gigabitethernet0/1
100.0.0.5	101.0.0.11	1	gigabitethernet0/1
100.0.0.5	101.0.0.12	1	gigabitethernet0/1
100.0.0.6	101.0.0.13	1	gigabitethernet0/1
100.0.0.6	101.0.0.14	1	gigabitethernet0/1
100.0.0.6	101.0.0.15	1	gigabitethernet0/1
100.0.0.6	101.0.0.16	1	gigabitethernet0/1

#View the dynamic blacklist entries generated by scanning on the Device.

```
Device#show blacklist ip lpu 0
Blacklist Info:
IpAddr,      CreateTime,      Agetime
-----
100.0.0.2   , Mon May 04 17:36:45 2021   , 94
```

---

### Note

- Both flood attack and scanning attack detection functions are only valid for local packets of the switch.
  - After specific attack source is identified for flood attack source tracing or scanning attack, it will be added to a dynamic blacklist with an aging time of 2 minutes. Before the blacklist ages, all packets of the attack source will be intercepted.
- 

## 96.3.4 Configure URPF Strict Mode

### Network Requirements

- PC accesses the IP Network through the Device. Configure URPF strict mode on the Device.
- PC simulates an attacker to send an illegal packet with a fake source address to access the IP Network, and the URPF function of the Device makes this packet discarded.

## Network Topology

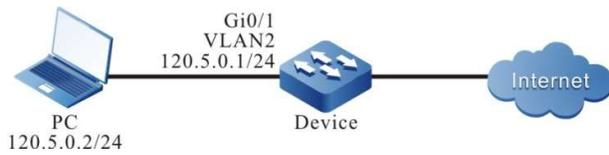


Figure 96 Network Topology for Configuring URPF Strict Mode

## Configuration Steps

Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configure the IP address and route of each interface, and require PC to access the IP Network through the Device. (Omitted)

Step 3: Configure URPF strict mode.

#Enable the URPF function on the Device, and configure URPF strict mode on the interface vlan2.

```
Device#configure terminal
Device(config)#ip urpf
Device(config)#interface vlan2
Device(config-if- vlan2)#ip urpf strict
Device(config-if- vlan2)#exit
```

Step 4: Check the result.

#PC accesses the IP Network through the Device. The source address is 120.5.0.2.

There is a route leading to 120.5.0.2 on the Device, and the output interface of the route is VLAN 2. The output interface of the route leading to the source address and the interface where the packet is received are the same interface VLAN2. After the URPF strict mode check, the packet is forwarded by the Device, and the PC can access the IP Network.

#PC simulates an attacker to send an illegal packet with a fake source address to access the IP Network through the Device. The source address is 120.10.0.2.

There is no route leading to 120.10.0.2 on the Device. URPF discards the packet, and PC cannot access the IP Network.

## 96.3.5 Configure URPF Loose Mode

### Network Requirements

- In the network environment, PC1 accesses PC2 through Device1, Device2 and Device3, and the response packets of PC2 reach PC1 through Device3 and Device1.
- Configure URPF loose mode on Device3.
- PC1 simulates an attacker to send an illegal packet with a fake source address to access PC2, and the URPF function of Device3 makes this packet discarded.

## Network Topology

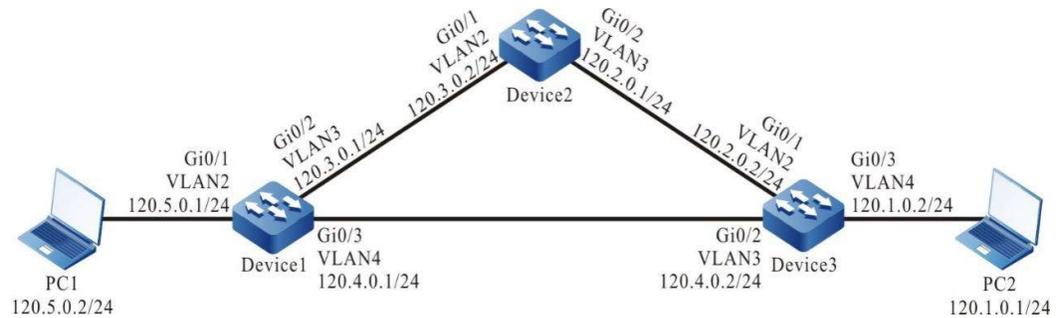


Figure 96 Network Topology for Configuring URPF Loose Mode

## Configuration Steps

- Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)
- Step 2: Configure IP addresses for the ports. (Omitted)
- Step 3: Configure static route in the network so that PC1 accesses PC2 through Device1, Device2 and Device3, and the response packets of PC2 reach PC1 through Device3 and Device1.

#Configure static route of Device1, Device2 and Device3, and build a network environment according to the network requirements.

```
Device1#configure terminal
Device1(config)#ip route 120.1.0.0 255.255.255.0 120.3.0.2
Device1(config)#ip route 120.2.0.0 255.255.255.0 120.3.0.2

Device2#configure terminal
Device2(config)#ip route 120.1.0.0 255.255.255.0 120.2.0.2

Device3#configure terminal
Device3(config)#ip route 120.5.0.0 255.255.255.0 120.4.0.1
```

#View the routing table of Device1, Device2 and Device3.

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS
```

Gateway of last resort is not set

```
S 120.1.0.0/24 [1/10] via 120.3.0.2, 00:10:49, vlan3
S 120.2.0.0/24 [1/10] via 120.3.0.2, 00:11:19, vlan3
C 120.3.0.0/24 is directly connected, 00:19:15, vlan3
C 120.4.0.0/24 is directly connected, 00:15:00, vlan4
C 120.5.0.0/24 is directly connected, 00:07:36, vlan2
C 127.0.0.0/8 is directly connected, 357:23:02, lo0
```

Device2#show ip route

Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management  
D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

```
S 120.1.0.0/24 [1/10] via 120.2.0.2, 00:15:37, vlan3
C 120.2.0.0/24 is directly connected, 00:17:17, vlan3
C 120.3.0.0/24 is directly connected, 00:25:21, vlan2
C 127.0.0.0/8 is directly connected, 00:38:29, lo0
```

Device3#show ip route

Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management  
D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

```
C 120.1.0.0/24 is directly connected, 00:17:01, vlan4
C 120.2.0.0/24 is directly connected, 00:19:13, vlan2
C 120.4.0.0/24 is directly connected, 00:18:50, vlan3
S 120.5.0.0/24 [1/10] via 120.4.0.1, 00:17:19, vlan3
C 127.0.0.0/8 is directly connected, 00:26:16, lo0
```

Step 4: Configure URPF loose mode on Device3.

#Enable the URPF function on Device3, and configure URPF loose mode on the vlan interface 2.

```
Device3#configure terminal
Device3(config)#ip urpf
Device3(config)#interface vlan 2
Device3(config-if-vlan2)#ip urpf loose
```

Device3(config-if-vlan2)#exit

Step 5: Check the result.

#PC1 ping PC2

The ping request packet of PC1 reaches PC2 through Device1, Device2 and Device3; the response packets of PC2 reach PC1 through Device3 and Device1.

#PC1 accesses PC2. The source address is 120.5.0.2.

There is a route leading to 120.5.0.2 on Device3, and the output interface of the route is VLAN3. Although the output interface VLAN 3 of the route leading to the source address and the interface VLAN 2 where the packet is received are different, after the URPF loose mode check, the packet is forwarded by Device3, PC1 can access PC2, and the response packet of PC2 reaches PC1 through Device3 and Device1.

#PC1 simulates an attacker to send an illegal packet with a fake source address to access PC2. The source address is 120.10.0.2.

There is no route leading to 120.10.0.2 on Device3. URPF discards the packet, and PC1 cannot access PC2.

---

## Note

- The packet discarding as a result of this detection will not generate any log or statistical information.
  - The URPF strict and loose modes are different in the following aspect: in loose mode, URPF searches routing table for the source IP address which receives packet, and permits this packet to pass if it is found; in strict mode, the packet is permitted to pass only when the route is found and its output interface is the same as the packet receiving interface.
  - Generally, the strict mode is applied. Loose mode is applied to the network environment with "inconsistent incoming and outgoing paths" in similar cases.
-

# 97 AARF

---

## 97.1 Overview

Anti Attack Resilient Framework is called AARF for short.

## 97.2 Introduction

In the network environment, switches are often attacked by malicious packets (e.g. ARP and ICMP). These attacks cause a heavy burden on the switch system, bring it to stop. Generally, too many packets will consume the CPU utilization, memory, entries or other resources of the switch so that the system cannot process other normal protocol and management packets. Sometimes, they may even cause suspended operation of the entire network.

AARF can effectively identify attacks and prevent the switch from being attacked. When the switch is attacked, it can ensure the normal operation of the system and protect the CPU from excessive load so that the entire network can operate normally.

## 97.3 Principle

Generally, it prevents the attack of protocol packets by counting the packets sent to CPU, calculating their sending rates, and compare them with the attack threshold value set. If the rate has reached the threshold value, it is considered that the packet is offensive, and the host with such offensive behavior will be limited, such as discarding CPU, limiting speed and filter, so as to protect the CPU.

As a matter of fact, different anti-attack functions for protocol packets use the same way to implement packet counting, identification and attack policy application. We can build an AARF by abstracting the same processing methods. AARF is used to implement some common processing mechanisms of the

anti-attack module to improve the extensibility of this module and reduce the workload in developing new module.

Currently, AARF supports arp-guard.

## 97.4 ARP-guard

ARP-guard is used to monitor the ARP packets on CUP in real time so as to prevent too many ARP packets from impacting the CPU and improve device security.

ARP-guard has three functions, i.e. ARP-guard based on host, ARP-guard based on port, and ARP scanning and identification.

The ARP-guard based on host counts the number of ARP packets received and compares the value with the threshold value set. If it exceeds the threshold value, they are identified as overspeed or offensive. Statistics and identification are based on either source IP address/VLAN ID/port or link layer source MAC address/VLAN ID/port.

The ARP-guard based on port counts the number of ARP packets that are received by the port and don't attack the host. If the value exceeds the threshold value set on the port, they are identified as overspeed or offensive. Port statistics exclude the ARP packets that have been identified as offensive for the host (host entries are generated and attack protection policy is applied).

ARP scanning and identification can identify ARP scanning with fixed MAC address yet constantly changing source IP, or that with fixed IP yet constantly changing destination IP.

### 97.4.1 ARP-guard Function Configuration

Table 97 ARP-guard Function Configuration List

Configuration Task	
Configure Basic Functions of ARP-guard	Enable Global ARP-guard Function
	Enable ARP-guard Function of the Port
Configure ARP-guard Monitoring Policy	Configure Global Monitoring Policy
	Configure Port Monitoring Policy

## 97.4.2 Configure Basic Functions of ARP-guard

The ARP-guard function based on port can take effect only after the global ARP-guard function is enabled.

### Configuration Condition

None

### Enable Global ARP-guard Function

Table 97 Enabling Global ARP-guard Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the AARF configuration mode	<b>aarf</b>	-
Enable Global ARP-guard Function	<b>arp-guard enable</b>	Mandatory By default, the ARP-guard function is disabled globally.

### Enable ARP-guard Function of the Port

Table 97 Enabling ARP-guard Function of Port

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the L2/L3 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected. After you enter the layer-2/3 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the
Enter Aggregation Group Configuration Mode	<b>link-aggregation</b> <i>link-aggregation-id</i>	

Step	Command	Description
		subsequent configuration takes effect only within the aggregation group.
Enable ARP-guard Function of the Port	<b>aarf arp-guard enable</b>	Mandatory By default, the ARP-guard function is disabled on the port.

### 97.4.3 Configure ARP-guard Monitoring Policy

#### Configuration Condition

No.

#### Configure Global ARP-guard Monitoring Policy

Table 97 Configuring Global ARP-guard Monitoring Policy

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the AARF configuration mode	<b>aarf</b>	-
Configure global ARP-guard monitoring policy	<b>arp-guard policy { filter   monitor   punish macbased}</b>	By default, the global ARP-guard monitoring policy is monitor.

#### Configure ARP-guard Monitoring Policy for Port

Table 97 Configuring ARP-guard Monitoring Policy for Port

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Enter the L2/L3 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2/3 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>link-aggregation</b> <i>link-aggregation-id</i>	
Configure ARP-guard monitoring policy for port	<b>aarf arp-guard policy</b> <b>{ filter   monitor  </b> <b>punish macbased}</b>	By default, the ARP-guard monitoring policy for port is not configured. The global ARP-guard monitoring policy is considered as the valid value.

The command **aarf arp-guard policy filter** is the host filtering protection policy under the port applied to the host or port with ARP attack behavior. After the filtering policy is configured, the host with ARP overspeed or attack behavior under the port will generate attack alarm. If the host sends ARP at a rate between the speed limit and attack threshold value, the rate of sending ARP packet to CUP will be limited to the speed limit, and the ARP packet in the forwarding direction will be forwarded at a host sending rate; if the rate of sending ARP by the host exceeds the attack threshold value, the ARP packet sent to CUP and forwarded will be discarded. If any overspeed or attack behavior is detected on the port (i.e. the total rate of receiving ARP packets that do not attack the host by the port is no less than the port rate limit or attack threshold value), an attack alarm will be generated. If the total rate of such ARP packets received by the port is between the port rate limit and the attack threshold value, it will limit the speed of the ARP packets sent to CPU according to the port rate limit, and the ARP packets to be forwarded will be forwarded at the original rate; If the total rate of such ARP packets received by the port is no less than the port attack threshold value, all ARP packets received by the port will be discarded in the forwarding direction and will not be sent to CPU.

The command **aarf arp-guard policy monitor** is the host monitoring protection policy under the port applied to the host or port with ARP attack behavior. After the monitoring policy is configured, if any host packets or port with ARP overspeed or attack behavior are detected under the port, an attack alarm will be generated, and the packets will be sent to CPU at the rate limit, with the ARP packets that exceed the rate limit being discarded by CPU; the ARP packets to be forwarded will be forwarded at the original rate.

The command **aarf arp-guard policy punish macbased** is the punishment-based rate limit protection policy under the port applied to the MAC host with ARP attack behavior. After the punishment-based rate limit policy is configured, when the MAC host packets with ARP overspeed or attack behavior are detected under the port, an attack alarm will be generated. If the rate of packets sent by the MAC host is between the rate limit and the attack threshold value, it will take effect according to the monitor policy. If the ARP packet rate is no less than the attack threshold value, the MAC packets attacking the host will be sent to CPU and forwarded at the rate which is half of the MAC rate limit. If the attack stops or the rate drops below the MAC rate limit, the host protection policy will be cancelled when the aging period expires. In addition, under this policy mode, both the port and IP host use the monitor policy.

#### 97.4.4 ARP-guard Monitoring and Maintaining

Table 97 ARP-guard Monitoring and Maintaining

Command	Description
<b>show aarf arp-guard configure</b>	Show the configuration of ARP-guard.
<b>show aarf arp-guard hosts</b>	Show the information of the monitored host.
<b>show aarf arp-guard ports</b>	Show the information of the monitored port.
<b>show aarf arp-guard scan</b>	Show the information of the scanning host.

### 97.5 Typical Configuration Example of AARF ARP-GUARD

#### 97.5.1 Configure Basic Functions of AARF ARP-GUARD

##### Network Requirements

- PC1, PC2 and PC3 access IP network through the Device.
- PC1 sends ARP packets to attack the Device which turns on AARF ARP-Guard and normally identifies ARP overspeed, ARP attack, ARP MAC scanning and ARP MAC-IP scanning so that the anti-attack policy takes effect.

##### Network Topology

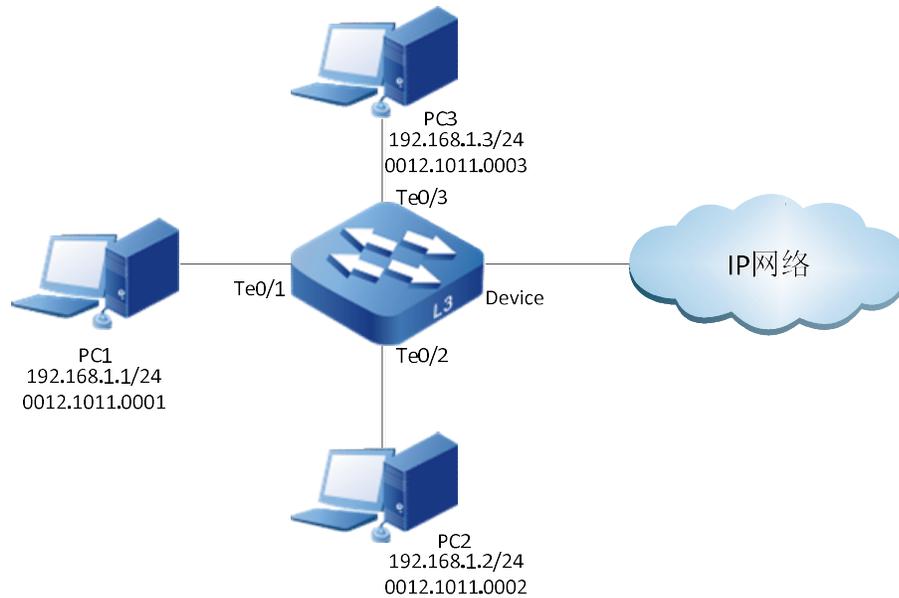


Figure 97-1 Network Topology for Configuring ARP-guard Function

### Configuration Steps

Step 1: Configure VLAN and port link type on Device.

#Create VLAN 2.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the link type of ports tengigabitethernet0/1, tengigabitethernet0/2 and tengigabitethernet0/3 as Access to allow services of VLAN2 to pass.

```
Device(config)#interface tengigabitethernet 0/1-0/3
Device(config-if-range)#switchport mode access
Device(config-if-range)#switchport access vlan 2
```

Step 2: Configure the gateway of PC1, PC2 and PC3 on the Device.

#Configure VLAN interface 2 as the gateway of PC1, PC2 and PC3

```
Device(config)#interface vlan 2
Device(config-if-vlan2)#ip address 192.168.1.254 24
```

Step 3: Configure AARF ARP-Guard on the Device.

#Globally enable AARF ARP-Guard

```
Device(config)#aarf
Device(config-aarf)#arp-guard enable
```

#Enable AARF ARP-Guard on the port tengigabitethernet0/1, relevant threshold value is default configuration, and the configuration policy is filter.

```
Device(config-if-tengigabitethernet0/1)# aarf arp-guard enable
Device(config-if-tengigabitethernet0/1)# aarf arp-guard policy filter
```

Step 4: Check the result.

#View AARF ARP-Guard-related configuration information

```
Device#show aarf arp-guard configure interface tengigabitethernet 0/1
(Format of column Rate-limit and Attack-threshold is per-src-ip/per-src-mac/per-interface.)
```

Interface/Global	Status	Rate-limit	Attack-threshold	Scan-threshold	Attack-policy
te0/1	Enabled	4/4/100	8/8/200	15	filter

#When the rate of ARP Request packets sent by PC1 to request the gateway IP address of the Device is no less than the host-based rate limit 4pps and less than the host-based attack threshold value 8pps, related entries will be formed and log information will be output, and the Device can identify the overspeed host-based ARP packets.

```
Device#show aarf arp-guard hosts
```

Interface	Vlan	IP	MAC
Action	Policy		
te0/1	2	192.168.1.1	-
overspeed	monitor		
te0/1	2	-	0012.1011.0001
overspeed	monitor		

Total: 2 record(s).

#Log output:

```
Dec 20 2016 03:45:28: %AARF-INTERFACE-3:<arp-guard>There are overspeed, attack or scan detected on interface
te0/1.(TUE DEC 20 03:45:25 2016)
Dec 20 2016 03:45:28: %AARF-DETECTED-3:<arp-guard>Host<IP=N/A,MAC=0012.1011.0001,interface=
te0/1,VLAN=2> overspeed was detected.(TUE DEC 20 03:45:25 2016)
Dec 20 2016 03:45:28: %AARF-DETECTED-3:<arp-guard>Host<IP=192.168.1.1,MAC=N/A,interface= te0/1,VLAN=2>
overspeed was detected.(TUE DEC 20 03:45:25 2016)
```

#When the rate of ARP Request packets sent by PC1 to request the gateway IP address of the Device is larger than the host-based attack threshold value 8pps, the Device will filter out these ARP packets, generate entries, output log information, and identify the host-based ARP packet attack.

```
Device#show aarf arp-guard hosts
```

Interface	Vlan	IP	MAC
Action	Policy		
te0/1	2	192.168.1.1	-
attack	filter		
te0/1	2	-	0012.1011.0001
attack	filter		

Total: 2 record(s).

#Log output:

```

Dec 20 2016 04:30:33: %AARF-INTERFACE-3:<arp-guard>There are overspeed, attack or scan detected on interface
te0/1.(TUE DEC 20 04:30:30 2016)
Dec 20 2016 04:30:33: %AARF-FILTER-3:<arp-guard>Host<IP=N/A,MAC=0012.1011.0001,interface=
te0/1,VLAN=2> attack was filter.(TUE DEC 20 04:30:30 2016)
Dec 20 2016 04:30:33: %AARF-FILTER-3:<arp-guard>Host<IP=192.168.1.2,MAC=N/A,interface=
te0/1,VLAN=2> attack was filter.(TUE DEC 20 04:30:30 2016)

```

#When PC1 sends several types of non-offensive ARP Request packets, and the sending rate is no less than the port-based rate limit 100 and less than the port-based attack threshold value 200, the Device will generate related entries, output log information, and identify the overspeed port-based ARP packets.

```

Device#show aarf arp-guard ports
-----
Interface          Hosts          Scan          Action
Policy
-----
te0/1              0              0              overspeed
  monitor

```

#Log output:

```

Dec 22 2016 06:36:32: %AARF-INTERFACE-3:<arp-guard>Interface te0/1 was overspeed.(THU DEC 22 06:36:29 2016)

```

#When PC1 sends several types of non-offensive ARP Request packets, and the sending rate is no less than the host-based attack threshold value 200, the Device will filter out all the ARP packets of this port, generate related entries, output log information, and identify the host-based ARP attack.

```

Device#show aarf arp-guard ports
-----
Interface          Hosts          Scan          Action
Policy
-----
te0/1              0              0              attack
  filter

```

#Log output:

```

Dec 22 2016 06:46:58: %AARF-INTERFACE-3:<arp-guard>Interface te0/1 was filter.(THU DEC 22 06:46:57 2016)

```

#When PC1 sends the ARP Request packets with source MAC unchanged and Sender IP increasing, and more than 15 ARP Request packets are sent within 10 seconds, the Device will generate related entries, output log information, and identify ARP MAC scanning.

```

Device#show aarf arp-guard scan
-----
Interface          Vlan          IP          MAC
                  Time-stamp
-----
te0/1              2              N/A          0012.1011.0001
THU DEC 22 03:16:30 2016
Total: 1 record(s).

```

#Log output:

```

Dec 22 2016 03:16:19: %AARF-INTERFACE-3:<arp-guard>There are overspeed, attack or scan detected on interface
te0/1.(THU DEC 22 03:16:16 2016)

```

Dec 22 2016 03:16:19: %AARF-SCAN-4:<arp-guard>Host<IP=N/A,MAC=0012.1011.0001,interface=te0/1,VLAN=2> scan was detected.(THU DEC 22 03:16:16 2016)

#When PC1 sends the ARP Request packets with both source MAC and Sender IP unchanged and Target IP increasing, and more than 15 ARP Request packets are sent within 10 seconds, the Device will generate related entries, output log information, and identify ARP MAC-IP scanning.

Device#show aarf arp-guard scan

```
-----  
Interface          Vlan          IP              MAC  
                   Time-stamp  
-----  
te0/1              2             192.168.1.254  0012.1011.0001 THU DEC 22  
03:38:52 2016  
Total: 1 record(s).
```

#Log output:

```
Dec 22 2016 03:37:33: %AARF-INTERFACE-3:<arp-guard>There are overspeed, attack or scan detected on interface te0/1.(THU DEC 22 03:37:30 2016)  
Dec 22 2016 03:37:33:%AARF-SCAN-4:<arp-guard>Host<IP=192.168.1.254,MAC=0012.1011.0001,interface=te0/1,VLAN=2> scan was detected.(THU DEC 22 03:37:30 2016)
```

# 98 PPPoE+

---

## 98.1 Introduction to Basic Functions of PPPoE+

PPPoE+ (Point-Point Protocol over Ethernet Plus) is also called PPPoE Intermediate Agent. Similar to DHCP option82, this function extends the PPPoE protocol packet. The access device identifies the client by intercepting the protocol packets in the PPPoE discovery phase, inserting the physical information of the client in the up direction, and peeling off the physical information of the client in the down direction.

## 98.2 Principle

- 1) The access device where the PPPoE+ function is enabled obtains the PADI packet sent by the PPPoE client. Then it adds the Vendor-Specific Tag to the load

- information field of the packet and sends it to the PPPoE server;
- 2) After receiving the PADI packet containing Vendor-Specific Tag, the PPPoE server will give the client PADO packet;
  - 3) The PPPoE client sends PADR packet upon receipt of PADO packet;
  - 4) When obtaining the PADR packet, the access device will add the Vendor-Specific Tag to the load information field of the packet and then send it to the PPPoE server;
  - 5) After receiving a PADR packet containing Vendor-Specific Tag, the PPPoE server will randomly generate a session-id, add it to the PADS packet field, and then send it to the PPPoE client. This can achieve the point-to-point PPP negotiation and PPPoE packet interaction with the client.

### 98.3 Vendor-Specific Tag for PPPoE Packet

This Tag is used to transmit the information defined by the manufacturer. In order that the PPPoE server can obtain the physical information of PPPoE client, Vendor-Specific Tag can be added to the PPPoE request packet.

When PPPoE packet interaction happens on the device, some user-related device information can be added to the PPPoE request packet through Vendor-Specific Tag. The Vendor-Specific Tag records the physical information of the client. Circuit-id is circuit ID, and remote-id is remote ID.

When the PPPoE+ function is enabled, after the device receives the PPPoE request packets, it may process them by the following manners according to the processing policy and fill method of Vendor-Specific Tag of PPPoE packet configured by users:

Table 98-1 PPPoE Request Packet Processing Policy

PPPoE request packet	Processing policy	Fill method	Packet processing principle
Without Vendor-Specific Tag	Add	Default fill format	Fill and forward in default format
	Add	Extend fill format	Fill and forward in the user-defined format
With Vendor-Specific Tag	maintained	Not filled	No processing or forwarding of PPPoE packet
	Filter	Discard the packet	Discard the packet

	Replacements	Default fill format	Replace the original Vendor-Specific Tag content in default format and forward
		Extend fill format	Replace the original Vendor-Specific Tag in the user-defined format and forward

## 98.4 Configure Basic Functions of PPPoE+

Table 98 PPPoE+ Function Configuration List

Configuration Task	
Configure to Enable/Disable PPPoE+ Function	Configure to Enable/Disable PPPoE+ Function of Port
Configure Processing Policy of PPPoE+ Function for PPPoE Packet with Vendor-Specific Tag	Configure Processing Policy of PPPoE+ Function for PPPoE Packet with Vendor-Specific Tag
Configure Content of Circuit-id in Vendor-Specific Tag	Configure Content of Circuit-id in Vendor-Specific Tag
Configure Content of Remote-id in Vendor-Specific Tag	Configure Content of Remote-id in Vendor-Specific Tag
Configure Fill Policy of PPPoE+ Function for Vendor-Specific Tag Contained in PPPoE Packet	Configure Fill Policy of PPPoE+ Function for Vendor-Specific Tag Contained in PPPoE Packet
Configure to Fill Value of Vendor-id in Vendor-Specific Tag	Configure to Fill Value of Vendor-id in Vendor-Specific Tag

### 98.4.1 Configure to Enable/Disable PPPoE+ Function

#### Configuration Condition

None

### Enable/disable PPPoE+ function

Table 98 Configuring to Enable/Disable PPPoE+ Function

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter layer-2 Ethernet interface mode	interface <i>interface name</i>	Enable/disable PPPoE+ under the mode
Enter the port aggregation group	interface link-aggregation <i>link-aggregation-id</i>	Enable/disable PPPoE+ function under the aggregation group mode
Enable/disable PPPoE+ function	pppoe relay enable/no pppoe relay enable	By default, the PPPoE+ function is disabled.

## 98.4.2 Configure Processing Policy of PPPoE+ Function for PPPoE Packet with Vendor-Specific Tag

### Configuration Condition

None

### Configure Processing Policy of PPPoE+ Function for PPPoE Packet with Vendor-Specific Tag

Table 98 Configuring Processing Policy of PPPoE+ Function for PPPoE Packet with Vendor-Specific Tag

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter layer-2 Ethernet interface mode	interface <i>interface name</i>	The configuration takes effect under the port mode only

Enter the port aggregation group	interface link-aggregation <i>link-aggregation-id</i>	The configuration takes effect under the aggregation group mode only
Configure the processing policy for PPPoE packet with Vendor-Specific Tag	pppoe relay information policy {keep drop replace}	By default, it is replace, i.e. replace and forward the packet field containing Vendor-Specific Tag.

### Note

- The command `pppoe relay information policy keep` is used to forward the PPPoE packet containing Vendor-Specific Tag as is under the port/aggregation group mode.
- The command `pppoe relay information policy drop` is used to discard the PPPoE packet containing Vendor-Specific Tag under the port/aggregation group mode.
  - The command `pppoe relay information policy replace` is used to replace and forward the Vendor-Specific Tag of PPPoE packet under the port/aggregation group mode.

## 98.4.3 Configure Content of Circuit-id in Vendor-Specific Tag

### Configuration Condition

None

### Configure Content of Circuit-id in Vendor-Specific Tag

Table 98 Configuring Content of Circuit-id in Vendor-Specific Tag

Step	Command	Description
Enter the global configuration mode.	<code>configure terminal</code>	-
Enter layer-2 Ethernet interface mode	interface <i>interface name</i>	The configuration takes effect under the port mode only.

Enter the port aggregation group	Interface link-aggregation <i>link-aggregation-id</i>	The configuration takes effect under the aggregation group mode only.
Configure the content of circuit-id	pppoe relay information format circuit-id{ <i>LINE</i>  default}	By default, fill vlan-interface in the packet.

### Note

- The command pppoe relay information format circuit-id *LINE* is used to allow users to configure the content of circuit-id.
  - The command pppoe relay information format circuit-id default is used to configure circuit-id to be filled with vlan-interface.

## 98.4.4 Configure Content of Remote-id in Vendor-Specific Tag

### Configuration Condition

None

### Configure Content of Remote-id in Vendor-Specific Tag

Table 98 Configuring Content of Remote-id in Vendor-Specific Tag

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter layer-2 Ethernet interface mode	interface <i>interface name</i>	The configuration takes effect under the port mode only.
Enter the port aggregation group	interface link-aggregation <i>link-aggregation-id</i>	The configuration takes effect under the aggregation group mode only.

Configure the content of remote-id	pppoe relay information format remote-id{ <i>LINE</i>  default }	By default, the mac address of the device port is filled in the packet.
------------------------------------	--	---

### Note

- The command pppoe relay information format remote-id *LINE* is used to allow users to configure the content of remote-id.
- The command pppoe relay information format remote-id default is used to configure circuit-id to be filled with switch-mac.

## 98.4.5 Configure Fill Policy of PPPoE+ Function for Vendor-Specific Tag Contained in PPPoE Packet

### Configuration Condition

None

### Configure Fill Policy of PPPoE+ Function for Vendor-Specific Tag Contained in PPPoE Packet

Table 98 Configuring Fill Policy of PPPoE+ Function for Vendor-Specific Tag Contained in PPPoE Packet

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter layer-2 Ethernet interface mode	interface <i>interface name</i>	The configuration takes effect under the port mode only
Enter the port aggregation group	interface link-aggregation <i>link-aggregation-id</i>	The configuration takes effect under the aggregation group mode only

Configure Fill Policy for Vendor-Specific Tag Contained in PPPoE Packet	pppoe relay information encapsulation {circuit-id remote-id both}	By default, circuit-id and remote-id are filled with default values.
---	---	--

#### 98.4.6 Configure to Fill Value of Vendor-id in Vendor-Specific Tag

##### Configuration Condition

None

##### Configure to Fill Value of Vendor-id in Vendor-Specific Tag

Table 98 Configuring Value of Circuit-id in Vendor-Specific Tag

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter layer-2 Ethernet interface mode	Interface <i>interface name</i>	The configuration takes effect under the port mode only
Enter the port aggregation group	interface link-aggregation <i>link-aggregation-id</i>	The configuration takes effect under the aggregation group mode only
Configure value of vendor-id	pppoe relay information vendor-id <i>vendor-id</i>	The value range is 0-4294967295. By default, the value of vendor-id is 2011.

# 99 HA

---

## 99.1 Overview

HA (High Availability) is one high availability management platform on the device, and it provides the regular detection for some system faults, ensuring that the services are not interrupted.

## 99.2 HA Function Configuration

### 99.2.1 HA Monitoring and Maintaining

Table 99 HA Monitoring and Maintaining

Command	Description
<b>show ham job</b>	Show current HA task processing table of local device

# 100 ULFD

---

## 100.1 Overview

In the traditional Ethernet, we usually use the fiber and other physical medium to connect the devices. In the actual networking, the fiber crossover connection (Figure 2-1), or one fiber not connected or disconnected (Figure 2-2) may result in the uni-directional communication. This kind of faulty link is called uni-directional link. The uni-directional link causes a series of problems. For example, the spanning tree detection failure results in the topology calculation error.

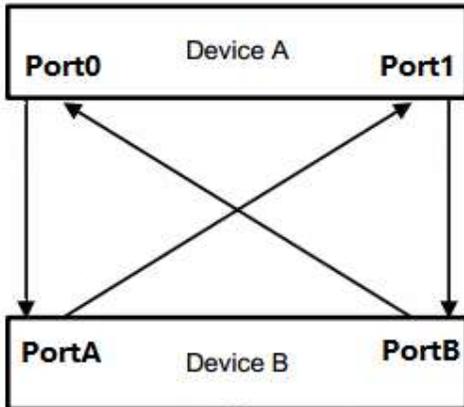


Figure 100 Fiber Cross-Connect

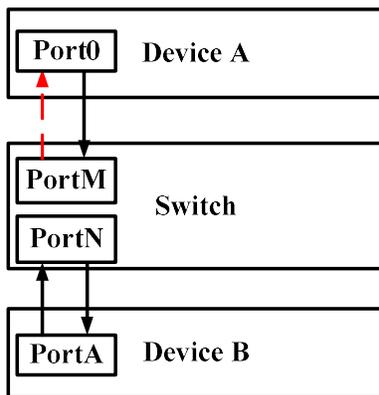


Figure 1 A Fiber not Connected or Disconnected

ULFD (Unidirectional Link Fault Detection) can monitor whether the fiber or twisted-pair has the uni-directional link. When ULFD detects the uni-directional link, it is responsible for closing the physical and logical uni-directional connection, sending the alarm information to the user and blocking the failure of other protocols.

## 100.2 ULFD Function Configuration

Table 100 ULFD Function Configuration List

Configuration Task	
Configure ULFD Basic Functions	Enable global ULFD function
	Enable the port ULFD function
Configure ULFD Parameters	Configure Sending Period of ULFD Detection Packet
	Reset Port Disabled by ULFD

### 100.2.1 Configure ULFD Basic Functions

#### Configuration Condition

Before configuring the ULFD basic functions, complete the following task:

- Ensure that the ULFD detection port is connected normally

#### Enable Global ULFD Function

ULFD has two work modes, that is, normal and aggressive. For the two modes, the basis of judging the uni-directional link is different. The normal mode is often used to check the uni-direction caused by the crossover connection. The aggressive mode is used to check the uni-directional connection caused by the crossover connection or disconnection.

Table 100 Enabling Global ULFD Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Enable global ULFD function	<b>ulfd { aggressive   enable }</b>	Mandatory  By default, the global ULFD function is disabled.

### Enable the Port ULFD Function

ULFD detection needs to enable the global ULFD detection function and the port ULFD detection function. If the ULFD function is not enabled globally, but just enabled on the port, the ULFD function cannot take effect.

If the global enabled ULFD detection mode and port enabled ULFD detection mode are inconsistent, the port ULFD detection mode takes effect first.

Table 1 Enabling Ethernet ULFD Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2/3 Ethernet interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Enable the port ULFD function	<b>ulfd port [ aggressive ]</b>	Mandatory  By default, the Ethernet ULFD function is disabled.

### Note

- To switch over the ULFD work mode on the port, first cancel the previous work mode and then configure the new mode.
- When enabling the ULFD function on the port, ensure that the neighbor port is also configured with the ULFD function and works in the same detection mode.

## 100.2.2 Configure ULFD Parameters

### Configuration Condition

Before configuring the ULFD parameters, first complete the following task:

- Enable the ULFD function

### Configure Sending Period of ULFD Detection Packet

ULFD periodically sends the detection packets to detect whether the network has the uni-directional link. We can modify the sending period of the detection packets according to the actuality of the network. The sending period of the detection packets is 7-90s. By default, it is 15s.

Table 100 Configuring Sending Period of ULFD Detection Packet

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the sending period of ULFD packet	<b>ulfd message time</b> <i>time-value</i>	Optional By default, the sending period of uni-directional detection packets is sent is 15 seconds.

### Reset Port Disabled by ULFD

If ULFD detects the uni-direction and disables the port and we want to re-enable the ULFD detection function of the port, the user needs to perform the reset operation manually. The operation sets the port to UP and re-enables the ULFD detection.

Table 2 Resetting Port Disabled by ULFD

Step	Command	Description
Reset Port Disabled by ULFD	<b>ulfd reset</b> [ <b>interface</b> <i>interface-name</i> ]	Optional By default, the Ethernet port cannot automatically reset after it is disabled.

## 100.2.3 ULFD Monitoring and Maintaining

Table 3 ULFD Monitoring and Maintaining

Command	Description
<code>show ulfd [ all   interface <i>interface-name</i> [ detail ] ]</code>	Show the global configuration information of ULFD and ULFD configuration of all/specified Ethernet ports

## 100.3 Typical Configuration Example of ULFD

### 100.3.1 Configure ULFD Basic Functions

#### Network Requirements

- Device1 is connected to Device2 through fiber.
- Configure aggressive ULFD to disable the port when a uni-directional link is detected.

#### Network Topology



Figure 2 Network Topology for Configuring Basic Functions of ULFD

#### Configuration Steps

Step 1: Configure ULFD functions.

#Enable ULFD functions on Device1, and configure ULFD mode as aggressive on the port gigabitethernet0/1.

```
Device1#configure terminal
Device1(config)#ulfd aggressive
Device1(config)#interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#ulfd port aggressive
Device1(config-if-gigabitethernet0/1)#exit
```

#Enable ULFD functions on Device2, and configure ULFD mode as aggressive on port gigabitethernet0/1.

```
Device2#configure terminal
Device2(config)#ulfd aggressive
Device2(config)#interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#ulfd port aggressive
Device2(config-if-gigabitethernet0/1)#exit
```

#View the ULFD information of port gigabitethernet0/1 on Device1.

```
Device1#show ulfd interface gigabitethernet 0/1
Interface name   : gigabitethernet0/1
ULFD config mode : Aggressive
ULFD running mode : Aggressive
Link status      : Link Up
Link direction   : Bidirectional
ULFD fsm status  : Advertisement
```

```
Neighbors number : 1
```

```
-----
Device ID       : 00017a787878
Interface name  : gigabitethernet0/1
Device Name     : Device2
Message Interval : 15
Timeout Interval : 5
Link Direction  : Bidirectional
Aging Time      : 40
Time to Die     : 36
-----
```

---

## Note

- The ULFD information of port on Device2 is viewed the same way as that on Device1. (Omitted)
- 

Step 2: Check the result.

#In the actual networking environment, as shown in Figure 2-1 and 2-2, when the fibers have crossover connection or a fiber is not connected or disconnected, uni-directional communication will happen. After the ULFD function is configured, when uni-directional communication is detected on Device1, port gigabitethernet0/1 will be closed and the following log information will be output:

```
%ULFD_LOG_WARN: gigabitethernet0/1: detected Unidirectional neighbor: device ID[00017a787878], device name[Device2], interface name[gigabitethernet0/1]!
```

```
%LINK-INTERFACE_DOWN-3: interface gigabitethernet0/1, changed state to down
```

```
%ULFD-UNDIR_LINK_ERR_V3-4: ULFD shutdown interface gigabitethernet0/1 successful
```

#It is indicated that port gigabitethernet0/1 is disabled.

```
Device1#show interface gigabitethernet 0/1
```

```
gigabitethernet0/1 configuration information
```

```
Description   :
Status        : Enabled
Link          : Down (Err-disabled)
Set Speed     : Auto
Act Speed     : Unknown
Def Speed     : Auto
Set Duplex    : Auto
Act Duplex    : Unknown
Def Duplex    : Auto
Set Flow Control : Off
Act Flow Control : Off
Mtu           : 1824
Port mode     : LAN
Port ability  : 100M FD,1000M FD
Link Delay    : No Delay
```

Storm Control : Unicast Disabled  
Storm Control : Broadcast Disabled  
Storm Control : Multicast Disabled  
Storm Action : None  
Port Type : Nni  
Pvid : 1  
Set Medium : Fiber  
Act Medium : Fiber  
Single-fiber : Disable  
Mac Address : 0000.1111.2224

---

## Note

- When configuring the ULFD function, ensure that the ULFDs at both ends of the link are working in the same detection mode.
  - For normal ULFD, please refer to this configuration method. Normal mode only supports the detection of uni-directional communication caused by fiber cross connect.
-

# 101 EIPS

---

## 101.1 Overview

In the layer-2 Ethernet, STP protocol is generally used for network reliability. As a standard ring protection protocol developed by IEEE, it has been widely applied. However, this protocol has been restricted by network size, and the convergence time is affected by network topology. Generally, STP has a second-level convergence time which increases with the growth of network diameter.

In order to reduce the convergence time and eliminate the influence of network size, EIPS (Ethernet Intelligent Protection Switching) technology is born. EIPS is a link layer protocol dedicated for Ethernet ring. It can prevent the broadcast storm caused by data loop in the Ethernet ring; when a link on the Ethernet ring is disconnected, the backup link can be quickly enabled to restore the communication between nodes on the ring network. Compared to STP protocol, EIPS is characterized by fast topological convergence (less than 50ms) and no relation between convergence time and the number of nodes on the ring network.

EIPS technology supports two modes, i.e. subring and hierarchy segment. In subring mode, two crossed rings are broken up into a main ring and a subring, and there is a common link between them; in the mode of hierarchy segment, when processing two crossed rings, one of them is selected as a main ring, and the ring on the main ring with the common link part shared with the main ring removed becomes a low-level link. Simply put, the subring mode splits the crossed rings into a main ring and a subring, while the hierarchy segment mode splits the crossed rings into a main ring and a low-level link. There is only one main ring, yet multiple subrings or low-level links.

### 101.1.1 Basic Concepts

To better understand the basic concepts mentioned in this section, please refer to the typical topologies of subring mode and hierarchy segment mode below.

#### EIPS Domain

The interconnected devices with the same domain ID and same control VLAN constitute an EIPS domain. An EIPS domain may contain multiple EIPS rings, one main ring and the others subrings. The EIPS domain is composed of the following elements: EIPS ring, EIPS control VLAN, master node, transmission node, edge control node, and assistant edge node.

#### EIPS Ring

EIPS ring is identified by integer IDs. It physically corresponds to a ring-shaped Ethernet topology. There is only one main ring and multiple subrings. Subrings intersect with the main ring through edge nodes, and subrings intersect with each other through the main ring. The main ring is level 0, lower than subrings.

### **EIPS Mode**

The switches on the EIPS ring are called nodes, each of which is a unique domain ID and ring ID. Each node is connected to the ring via two ports. The master port and slave port are specified by the user.

**Master port:** It serves as both the initiator of ring network status polling and the decision maker of operation performance after the status of network topology is changed. There is only one master node on each ring.

**Transmission node:** All except master node on the master ring of EIPS are transmission nodes. Transmission nodes are responsible for monitoring the status of the link directly connected to them, and reporting the status change through EIPS protocol packet to the master node which makes decisions on how to process it.

The two nodes where subring and master ring intersect are called edge nodes (called transmission nodes on the master ring) that include edge control nodes and assistant edge nodes. These two types of nodes must be used in pair to detect the integrity or failure status of subring.

### **EIPS Control VLAN**

Control VLAN is used to transmit EIPS protocol packets. The port on the EIPS ring must be added to the control VLAN, and no IP address is permitted to configure on the control VLAN interface. In the subring mode, the port on master ring should be added to the control VLAN of both master ring and subring, and that on subring is required to be added to the control VLAN of subring only. In the hierarchy segment mode, the same VLAN on master ring and low-level segment can be used as control VLAN.

### **EIPS Port**

EIPS port is an abstract concept, which corresponds to a link makes up an EIPS ring. This link can be either a single physical link or an aggregation port composed of multiple physical links. Each EIPS node has two ports connected to EIPS ring. Since there are EIPS rings intersecting, an EIPS port may belong to multiple EIPS nodes.

**Master and secondary EIPS port:** There is master port and slave port on the master node and transmission nodes. The master port on the master node sends hello packet, and the slave port receives this packet. This can ensure the integrity of the loop. When the loop is complete, it is required to obstruct the data VLAN of the slave port on the master node. For transmission nodes, neither master port nor slave port has special meanings.

### **Topology Level**

Topology level means the ring hierarchical division of EIPS domain. EIPS domain is composed of one ring or several rings intersecting with each other. When there is a single ring in the domain, it is a major-level ring, numbered 0; when there are multiple rings intersecting with each other in the domain, one of them is

selected as a major-level ring, numbered 0, and the ring connected to this major-level ring with the common part shared with the major-level ring removed becomes a link in low-level segment.

Low-level link is the set of links with the common part connected to the upper layer removed.

The major-level ring has the highest level number (0). The lower the level, the larger the level number.

### **Topology Segment**

In EIPS, segment number is used to differentiate different low-level links in the same level. Multiple low-level links can appear in the same level of the domain. The multiple low-level links in the same level are defined with different segment numbers. In particular, the segment number of the major-level ring is 0.

After dividing levels and segments in the EIPS domain, corresponding ring or low-level ring in each level and segment has unique level and segment numbers, called level segment. The low-level link where level and segment numbers are defined are called low-level segments.

## **101.1.2 Operating Mechanism**

### **Polling Mechanism**

With the polling mechanism, the master node of EIPS ring actively detects the integrity of the ring network.

The master node periodically sends from its master port Hello packet which passes every transmission node and spread on the ring. If the loop is healthy, the slave port of the master node will receive Hello packet before time-out of the timer, and the master node will maintain the slave port obstructed. If the loop is broken so that the slave port of the master node cannot receive Hello packet before time-out of the timer, the master node will cancel the obstruction status of data VLAN on the slave port and send COMM-FLUSH-FDB packet to notify all transmission nodes so that they can update their forwarding entries.

### **Link Down Alarm Mechanism**

When the transmission node or edge node finds any of its port which belongs to EIPS ring becomes down, it will immediately send a Link-Down packet to the master node. After receiving the Link-Down packet, the master node will immediately cancel the obstruction status of data VLAN on the slave port and send COMM-FLUSH-FDB packet to notify all transmission and edge nodes so that they can update their forwarding entries. After the nodes update their entries, the data flow switch to the normal link.

### **Loop Recovery Mechanism**

When the port which belongs to EIPS ring on transmission node or edge node is up again, the master node may find loop recovery after a period of time. For data VLAN, there may be a temporary loop in the network and then broadcast storm during this period of time.

In order to avoid temporary loop, non-master node immediately obstructs the port connecting to the ring network (only permitting the packet of control VLAN to pass) once it finds this port is up again until it believes no loop will be generated.

## Load Balancing Mechanism

Load balancing is achieved by configuring multiple EIPS domains on the same ring network and permitting different EIPS domains to send traffic of different data VLANs, i.e. traffic of different VLANs is forwarded along different paths.

## Backup Master Node Mechanism

The transmission node directly connected to the slave port of the master node is considered as the backup master node. When the master node is normal, the backup master node works as a transmission node; when the master node crashes, the backup master node will continue to work on behalf of the master node.

### 101.1.3 Typical Topology of Subring Mode

#### Single Ring

Domain1 of EIPS domain has an EIPS ring Ring1, a master node Master, three transmission nodes Transit1, Transit2 and Transit3, as shown in the figure below.

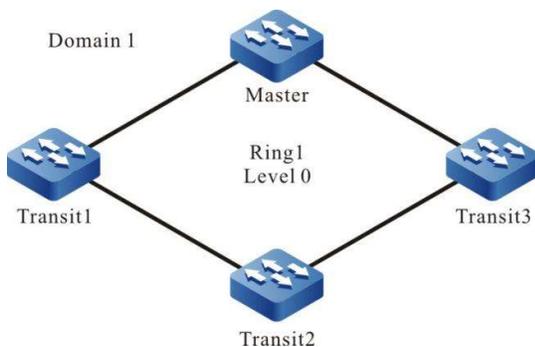


Figure 101 Topology of Single Ring

This networking is characterized by rapid response and short convergence time in case of topology change.

#### Typical Networking of Intersecting Rings

Domain1 of EIPS domain contains two EIPS rings, i.e. Ring1 and Ring2. In particular, Ring1 is the main ring, and Ring2 is the subring. The main ring Ring1 has a master node Master and two transmission nodes Transit1 and Transit2; the sub-ring Ring2 includes the edge control node Edge control (i.e. Transit3), assistant edge node Edge assistant (i.e. Transit4), transmission nodes Sub Transit1 and Sub Transit2, and edge nodes Edge control and Edge assistant that are also the transmission nodes of Ring1. This is shown in the image below.

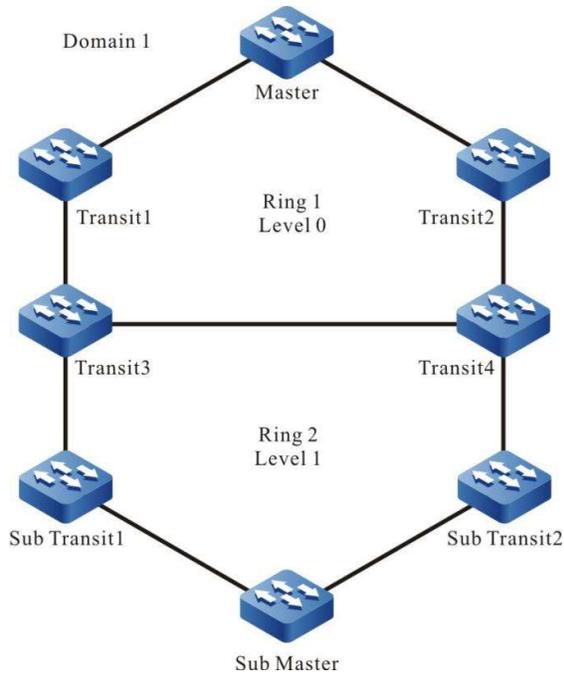


Figure 101 Typical Network Topology of Intersecting Rings

In this typical application of networking, subrings can be dual-homed to uplink with two edge nodes to provide uplink backup.

### 101.1.4 Typical Topology of Hierarchy Segment Mode

#### Single Ring

Domain1 of EIPS domain has an EIPS ring Ring1, a master node Master, and three transmission nodes Transit1, Transit2 and Transit3. Master port Primary and slave port Slave are configured on the master node. There is only one ring in Domain1. This single ring is defined as the major-level ring, the level as 0, and the segment as 0. When there is no fault in the major-level ring, EIPS blocks the data VLAN of the slave port Slave. This is shown in the image below.

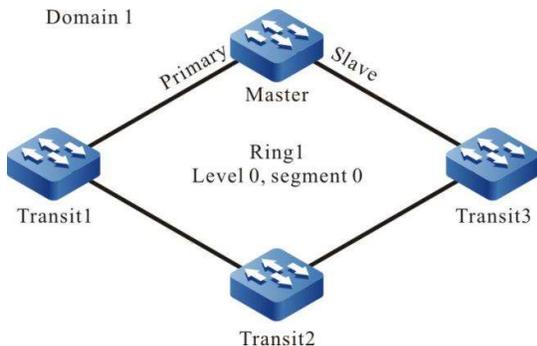


Figure 101 Topology of Single Ring in Hierarchy Segment Mode

## Topology of Intersecting Rings

There are rings intersecting in Domain1 which is decomposed into a hierarchical structure containing a major-level ring and a low-level segment. Both level and segment of main ring Ring1 are defined as 0; the ring intersecting with Ring1 becomes a low-level segment after removing the common part connected to Transit2 and Transit3, which is assigned level and segment numbers of 1.

The major-level ring (level 0, segment 0) contains a master node Master and four transmission nodes Transit1, Transit2, Transit3 and Transit4. It is a single ring. The low-level segment (Level 1, segment 1) has edge control node Edge control (i.e. Transit2) and assistant edge node Edge assistant (i.e. Transit3), and transmission nodes Transit5 and Transit6, as shown below.

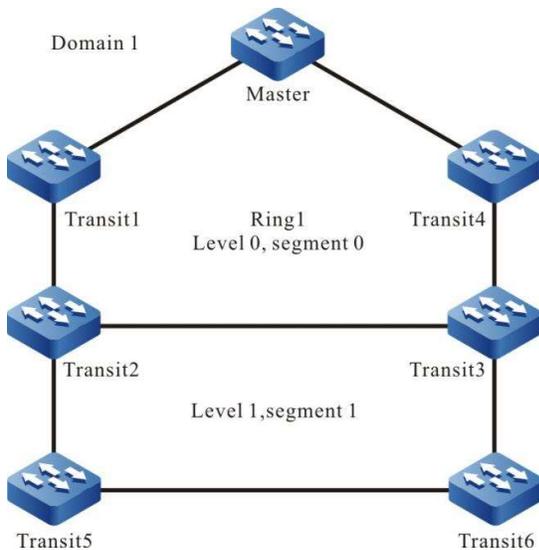


Figure 1 Topology of Intersecting in Hierarchy Segment Mode

## 101.2 EIPS Function Configuration

Table 101 EIPS Function Configuration List

Configuration Task	
Configure EIPS Ring	Configure EIPS Master Node
	Configure Transmission Node of EIPS
	Configure Edge Control Node of EIPS

	Configure Assistant Edge Node of EIPS
	Configure EIPS Domain
	Configure EIPS Control VLAN
	Configure EIPS Level Number
	Configure EIPS Segment Number
	Configure EIPS Data Instance
Configure EIPS Reliability	Configure EIPS Backup Master Node
	Configure EIPS uni-directional detection
Configure EIPS Timer	Configure EIPS Timer

## Note

- EIPS technology supports two modes, i.e. subring and hierarchy segment.
- Hierarchy segment mode is recommended.
- There is little difference between hierarchy segment mode and subring mode in configuration. In hierarchy segment mode, parameter **segment** must be used in creating various EIPS nodes, and EIPS segment number needs to be configured.

### 101.2.1 Configure EIPS Ring

When configuring EIPS ring, you are required to configure the ports that will access EIPS ring on each node and the nodes on the ring.

#### Configuration Condition

Before configuring EIPS ring, do the following:

- Configure the type of the ports to be added to each node as nni;
- Close the spanning tree protocol of the ports to be added to each node;
- Configure the ports to be added to each node as trunk mode;
- Add the ports to be added to each node to the control VLAN to which the node belongs.

#### Configure EIPS Master Node

Please configure the device to be configured as a master node as follows.

Table 1 Configuring EIPS Master Node

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Create EIPS master node	<b>eips ring <i>ring-id</i> master [ <i>segment</i> ]</b>	Mandatory By default, no EIPS master node is created.  Parameter <i>segment</i> is recommended to specify the EIPS ring network as hierarchy <i>segment</i> mode. Otherwise, it is <i>subring</i> mode.
Configure master port of the master node	<b>primary interface <i>interface-name</i></b>	Mandatory By default, master port of the master node is not configured.
Configure slave port of the master node	<b>secondary interface <i>interface-name</i></b>	Mandatory By default, slave port of the master node is not configured.
Configure data instance of the master node	<b>instance <i>instance-id</i></b>	Mandatory By default, data instance of the master node is not configured.  The data VLAN permitted by the EIPS port should be included in the EIPS data instance, and all nodes of the same EIPS domain should be configured with the same data instance.

---

 **Note**

- In subring mode, all ports on the main ring need to be added to the control VLAN of the subring.
- 

### Configure Transmission Node of EIPS

Please configure the device to be configured as a transmission node as follows.

Table 2 Configuring Transmission Node of EIPS

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Create transmission node of EIPS	<b>eips ring <i>ring-id</i> transit [ <i>segment</i> ]</b>	Mandatory By default, no transmission node of EIPS is created. Parameter <i>segment</i> is recommended to specify the EIPS ring network as hierarchy segment mode. Otherwise, it is subring mode.
Configure master port of the transmission node	<b>primary interface <i>interface-name</i></b>	Mandatory By default, master port of the transmission node is not configured.
Configure slave port of the transmission node	<b>secondary interface <i>interface-name</i></b>	Mandatory By default, slave port of the transmission node is not configured.
Configure data instance of the transmission node	<b>instance <i>instance-id</i></b>	Mandatory By default, data instance of the transmission node is not configured. The data VLAN permitted by the EIPS port should be

		included in the EIPS data instance, and all nodes of the same EIPS domain should be configured with the same data instance.
--	--	---

### Configure Edge Control Node of EIPS

Please configure the device to be configured as an edge control node as follows.

Table 3 Configuring Edge Control Node of EIPS

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure edge control node	<b>eips ring <i>ring-id</i> edge [ segment ]</b>	Mandatory By default, no edge control node is configured. Parameter segment is recommended to specify the EIPS ring network as hierarchy segment mode. Otherwise, it is subring mode.
Associate edge control node with transmission node	<b>transit ring <i>ring-id</i></b>	Mandatory By default, edge control node is not associated with transmission node. Only when the edge control node is associated with the transmission node, low-level segments or sub-rings can work together with the main ring
Configure edge port of edge control node	<b>edge interface <i>interface-name</i></b>	Mandatory By default, no edge port is designated for edge control node.

		Edge port is used to connect low-level segment or subring with main ring
Configure data instance of edge control node	<b>instance</b> <i>instance-id</i>	<p>Mandatory</p> <p>By default, no data instance is configured for edge control node.</p> <p>The data VLAN permitted by the EIPS port should be included in the EIPS data instance, and all nodes of the same EIPS domain should be configured with the same data instance.</p>

### Configure Assistant Edge Node of EIPS

Please configure the device to be configured as an assistant edge node as follows.

Table 4 Configuring Assistant Edge Node of EIPS

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure assistant edge node	<b>eips ring</b> <i>ring-id</i> <b>assistant</b> [ <b>segment</b> ]	<p>Mandatory</p> <p>By default, no assistant edge node is configured.</p> <p>Parameter segment is recommended to specify the EIPS ring network as hierarchy segment mode. Otherwise, it is subring mode.</p>
Associate assistant edge node with transmission node	<b>transit ring</b> <i>ring-id</i>	<p>Mandatory</p> <p>By default, assistant edge node is not associated with transmission node.</p> <p>Only when the assistant edge node is associated with the transmission node,</p>

		low-level segments or sub-rings can work together with the main ring
Configure edge port of assistant edge node	<b>edge interface</b> <i>interface-name</i>	Mandatory  By default, edge port of the assistant edge node node is not configured.  Edge port is used to connect low-level segment or subring with main ring
Configure data instance of assistant edge node	<b>instance</b> <i>instance-id</i>	Mandatory  By default, no data instance is configured for assistant edge node.  The data VLAN permitted by the EIPS port should be included in the EIPS data instance, and all nodes of the same EIPS domain should be configured with the same data instance.

### Configure EIPS Domain

Specify the domain to which the EIPS ring or hierarchy segment belongs, and configure all nodes in the same EIPS domain with the same domain ID.

Table 101 Configuring EIPS Domain

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the EIPS configuration mode	<b>eips ring</b> <i>ring-id</i> { <b>master</b>   <b>transit</b>   <b>edge</b>   <b>assistant</b> } [ <b>segment</b> ]	-
Configure EIPS Domain	<b>domain id</b> <i>domain-id</i>	Mandatory  By default, EIPS domain is not configured.

### Configure EIPS Control VLAN

Configure the control VLAN of EIPS ring or hierarchy segment; configure the control VLAN prior to enabling EIPS protocol; configure all nodes in the same EIPS ring with the same control VLAN. Therefore, when configuring control VLAN, please select a VLAN that has been created yet has not been used by other layer-2 protocols. Otherwise, the configuration cannot succeed.

EIPS control VLAN is used to transmit EIPS protocol packets. Data packets are not permitted to enter the control VLAN.

Table 101 Configuring EIPS Control VLAN

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the EIPS configuration mode	<b>eips ring <i>ring-id</i> { master   transit   edge   assistant } [ segment ]</b>	-
Configure EIPS Control VLAN	<b>control vlan <i>vlan-id</i></b>	Mandatory By default, no EIPS control VLAN is configured.

### Configure EIPS Level Number

EIPS level number is an important sign to distinguish main ring from subring or low-level segment. The level numbers of all main rings are 0, those of first-level subrings or hierarchy segments are 1, and so on. Node of subring must be configured, and the level numbers of subrings or hierarchy numbers at the same level must be the same.

Table 101 Configuring EIPS Level Number

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the EIPS configuration mode	<b>eips ring <i>ring-id</i> { master   transit   edge   assistant } [ segment ]</b>	-

Configure the level number of subring or hierarchy segment	<b>level</b> <i>level-id</i>	Mandatory  By default, level number is not configured for subring or hierarchy segment.
--	------------------------------	---

### Configure EIPS Segment Number

Segment number is an important sign in the hierarchy segment mode. The segment number of main ring is 0, and that of low-level segment is defined by users. The hierarchy segment with a level number greater than 0 must be configured with a segment number, and all nodes on the same hierarchy segment must have the same segment numbers.

Table 5 Configuring EIPS Number

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the EIPS configuration mode	<b>eips ring</b> <i>ring-id</i> { <b>master</b>   <b>transit</b>   <b>edge</b>   <b>assistant</b> } [ <b>segment</b> ]	-
Configure EIPS Segment Number	<b>segment</b> <i>segment-id</i>	Mandatory  By default, segment number is not configured for the hierarchy segment.  This command is exclusive for EIPS-level segment. The subring mode doesn't have this command. Segment number is configured on the edge control node, assistant edge node and transmission node of low-level segment.

### Configure EIPS Data Instance

Data instance is configured prior to configuring EIPS ring or hierarchy segment; the data VLAN permitted by the EIPS port should be included in the EIPS data instance; all nodes of the same EIPS domain should be configured with the same data instance.

Data instance is configured by referencing MSTP (Multiple Spanning Tree Protocol Instance). Therefore, before configuring EIPS ring or hierarchy segment, the mapping relationship between the MSTP instance and the VLAN to be included should be configured.

Table 6 Configuring EIPS Data Instance

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the MSTP configuration mode	<b>spanning-tree mst configuration</b>	-
Configure MSTP instance	<b>instance</b> <i>instance-id</i> <b>vlan</b> <i>vlan-range</i>	Mandatory  By default, MSTP creates instance 0 which contains all VLANs.  Configure MSTP and map to corresponding data VLAN
Activate MST domain parameter configuration.	<b>active configuration pending</b>	Mandatory  By default, MST domain parameters do not take effect immediately after modification unless this command is executed.
Enter the global configuration mode.	<b>exit</b>	-
Enter the EIPS configuration mode	<b>eips ring</b> <i>ring-id</i> { <b>master</b>   <b>transit</b>   <b>edge</b>   <b>assistant</b> } [ <b>segment</b> ]	-
Configure EIPS Data Instance	<b>instance</b> <i>instance-id</i>	Mandatory  By default, EIPS data instance is not configured.

### Enable EIPS Protocol

Upon completion of the configuration mentioned above, use this command to enable EIPS protocol.

Table 7 Enabling Protocol on EIPS Node

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the EIPS configuration mode	<b>eips ring <i>ring-id</i> { master   transit   edge   assistant } [ segment ]</b>	-
Enable EIPS protocol	<b>eips start</b>	Mandatory By default, EIPS protocol is not enabled on the node.

### 101.2.2 Configure EIPS Reliability

#### Configuration Condition

None

#### Configure EIPS Backup Master Node

In order to improve the reliability of EIPS ring network, the backup master node will replace the master node to perform its functions when the master node crashes.

The backup master node needs to be configured on the transmission node directly connected to the master node.

Table 8 Configuring EIPS Backup Master Node

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the EIPS configuration mode	<b>eips ring <i>ring-id</i> { master   transit   edge   assistant } [ segment ]</b>	-
Configure the specified transmission node as a backup master node	<b>backup master</b>	Mandatory By default, backup master node is not configured.

## Configure EIPS Uni-directional Detection

Enable the uni-directional function under the port or port group.

Table 9 Configuring EIPS Uni-directional Detection of Port

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	-
Configure EIPS uni-directional detection of port	<b>eips udd interval</b> [ <i>value</i> ]	Mandatory  By default, the uni-directional detection function is not disabled on the port.

## 101.2.3 Configure EIPS Timer

### Configuration Condition

Before configuring EIPS timer, do the following:

- Configure basic EIPS functions.

### Configure EIPS Timer

The master node and the edge control node in hierarchy segment mode use timer to control the frequency of sending hello packet and the timeout period of receiving hello packet, and the transmission node uses blocking timer to control the time taken for node to transform to complete state when the failure of transmission node recovers.

Table 10 Configuring EIPS Timer

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the EIPS configuration mode	<b>eips ring</b> <i>ring-id</i> { <b>master</b>   <b>transit</b>   <b>edge</b>   <b>assistant</b> } [ <b>segment</b> ]	-

Configure timer of EIPS node	<b>timer</b> { <b>hello</b>   <b>receive</b>   <b>block</b> } <i>timer-value</i>	Mandatory  By default, the timeout period of hello timer is 1 second, that of receive timer is 5 seconds, and that of block timer is 10 seconds.
------------------------------	--	--

## Note

- The timer for sending hello packet can be configured on the master node or edge control node only, and the blocking timer on the transmission node only.

## Caution

- If backup master node is configured, the timeout period of hello timer on master node cannot be configured as 0.

## 101.2.4 EIPS Monitoring and Maintaining

Table 11 EIPS Monitoring and Maintaining

Command	Description
<b>clear eips</b> { <b>interface</b> [ <i>interface-name</i> ]   <b>interface link-aggregation</b> [ <i>link-aggregation-number</i> ]   <b>ring</b> [ <i>ring-id</i> ]   <b>udld</b> }	Clear EIPS-related statistics
<b>show eips</b> { <b>config</b> [ <i>ring-id</i> ]   <b>interface</b> [ <i>interface-name</i> ]   <b>interface link-aggregation</b> [ <i>link-aggregation-number</i> ]   <b>mac-control-table</b>   <b>ring</b> [ <i>ring-id</i> ]   <b>ticktimer</b> [ <i>ticktime-name</i> ]   <b>topology</b> [ <i>ring ring-id</i> ]   <b>topology-summary</b> [ <i>ring ring-id</i> ]   <b>udld</b> [ <b>interface</b> <i>interface-name</i> ] }	Show the configuration, status and statistical information of EIPS. This includes EIPS port, aggregation port, address table, node, topology, timer-related information, and information related to UDLD uni-directional communication.

## 101.3 Typical Configuration Example of EIPS

### 101.3.1 Configure Single Ring in EIPS Hierarchy Segment Mode

#### Network Requirements

- There are four devices in Ring 1 of EIPS within LAN. Configure EIPS hierarchy segment mode, and protect the ring network by blocking the slave port gigabitethernet0/2 of Master node.
- When the link between transmission nodes Transit1 and Transit2 is disconnected, it can cancel the spanning tree blocking state of the Master node's slave port gigabitethernet0/2 so that data switch and the communication within the LAN are not affected.

#### Network Topology

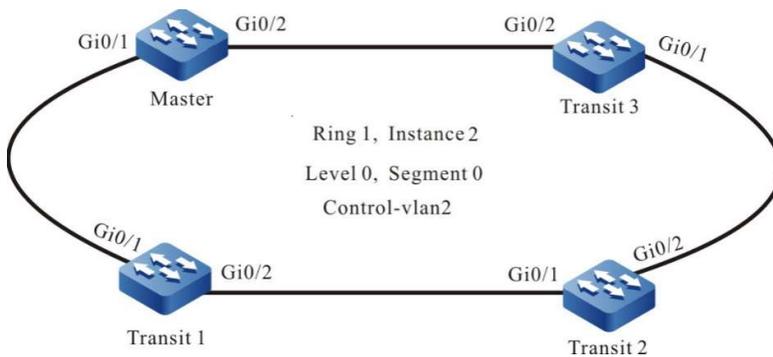


Figure 2 Network Topology for Configuring Single Ring in EIPS Hierarchy Segment Mode

#### Configuration Steps

Step 1: Configure VLANs, and configure the link type of the ports.

#On Master, create VLAN2 and VLAN3, and configure the link type of ports gigabitethernet0/1~gigabitethernet0/2 as Trunk, permitting services of VLAN2 and VLAN3 to pass. Configure PVID as 1.

```
Master#configure terminal
Master(config)#vlan 2-3
Master(config)#interface gigabitethernet 0/1-0/2
Master(config-if-range)#switchport mode trunk
Master(config-if-range)#switchport trunk allowed vlan add 2-3
Master(config-if-range)#switchport trunk pvid vlan 1
```

#On Master, map VLAN3 to the spanning tree instance 2, and close spanning tree and storm suppression functions on ports gigabitethernet0/1~gigabitethernet0/2.

```

Master (config)#spanning-tree mst configuration
%Alert: Commands configured under the mode would not take effect immediately, you should active them explicitly!
Master (config-mst)#instance 2 vlan 3
Master (config-mst)#active configuration pending
Master(config-if-range)#exit
Master(config)#interface gigabitethernet 0/1-0/2
Master(config-if-range)#no spanning-tree enable
Master(config-if-range)#no storm-control multicast
Master(config-if-range)#no storm-control unicast
Master(config-if-range)#no storm-control broadcast
Master(config-if-range)#exit

```

#On the transmission node Transit1, create VLAN2 and VLAN3, map VLAN3 to the spanning tree instance 2, configure the link type of ports gigabitethernet0/1~gigabitethernet0/2 as Trunk, permitting services of VLAN2 and VLAN3 to pass, and configure PVID as 1. Close spanning tree and storm suppression functions on ports gigabitethernet0/1~gigabitethernet0/2. (Omitted)

#On Transit2, create VLAN2 and VLAN3, map VLAN3 to the spanning tree instance 2, configure the link type of ports gigabitethernet0/1~gigabitethernet0/2 as Trunk, permitting services of VLAN2 and VLAN3 to pass, and configure PVID as 1. Close spanning tree and storm suppression functions on ports gigabitethernet0/1~gigabitethernet0/2. (Omitted)

#On the transmission node Transit3, create VLAN2 and VLAN3, map VLAN3 to the spanning tree instance 2, configure the link type of ports gigabitethernet0/1~gigabitethernet0/2 as Trunk, permitting services of VLAN2 and VLAN3 to pass, and configure PVID as 1. Close spanning tree and storm suppression functions on ports gigabitethernet0/1~gigabitethernet0/2. (Omitted)

---

## Note

- VLAN2 is a control VLAN used to transmit EIPS protocol packets, and VLAN3 is a data VLAN used to forward services.
  - To use the EIPS function, you must map the EIPS data VLAN to corresponding spanning tree instance, and disable the spanning tree function on the port.
- 

Step 2: Configure the EIPS hierarchy segment mode.

#On the master node Master, create master node Ring1 of the major ring in hierarchy segment mode, configure the level and segment number of EIPS ring as 0, instance of EIPS ring as 2, control VLAN as VLAN2, master port as gigabitethernet0/1 and slave port as gigabitethernet0/2, and enable EIPS.

```
Master(config)#eips ring 1 master segment
```

```
Master(config-eips)#control vlan 2
Master(config-eips)#level 0
Master(config-eips)#segment 0
Master(config-eips)#instance 2
Master(config-eips)#primary interface gigabitethernet 0/1
Master(config-eips)#secondary interface gigabitethernet 0/2
Master(config-eips)#eips start
Master(config-eips)#exit
```

#On the transmission node Transit1, create transmission node Ring1 in hierarchy segment mode, configure the level and segment number of EIPS ring as 0, instance of EIPS ring as 2, control VLAN as VLAN2, master port as gigabitethernet0/1 and slave port as gigabitethernet0/2, and enable EIPS.

```
Transit1(config)#eips ring 1 transit segment
Transit1(config-eips)#control vlan 2
Transit1(config-eips)#level 0
Transit1(config-eips)#segment 0
Transit1(config-eips)#instance 2
Transit1(config-eips)#primary interface gigabitethernet 0/1
Transit1(config-eips)#secondary interface gigabitethernet 0/2
Transit1(config-eips)#eips start
Transit1(config-eips)#exit
```

#On the transmission node Transit2, create transmission node Ring1 in hierarchy segment mode, configure the level and segment number of EIPS ring as 0, instance of EIPS ring as 2, control VLAN as VLAN2, master port as gigabitethernet0/1 and slave port as gigabitethernet0/2, and enable EIPS.

```
Transit2(config)#eips ring 1 transit segment
Transit2(config-eips)#control vlan 2
Transit2(config-eips)#level 0
Transit2(config-eips)#segment 0
Transit2(config-eips)#instance 2
Transit2(config-eips)#primary interface gigabitethernet 0/1
Transit2(config-eips)#secondary interface gigabitethernet 0/2
Transit2(config-eips)#eips start
Transit2(config-eips)#exit
```

#On the transmission node Transit3, create transmission node Ring1 in hierarchy segment mode, configure the level and segment number of EIPS ring as 0, instance of EIPS ring as 2, control VLAN as VLAN2, master port as gigabitethernet0/1 and slave port as gigabitethernet0/2, and enable EIPS.

```
Transit3(config)#eips ring 1 transit segment
Transit3(config-eips)#control vlan 2
Transit3(config-eips)#level 0
Transit3(config-eips)#segment 0
Transit3(config-eips)#instance 2
```

```

Transit3(config-eips)#primary interface gigabitethernet 0/1
Transit3(config-eips)#secondary interface gigabitethernet 0/2
Transit3(config-eips)#eips start
Transit3(config-eips)#exit

```

Step 3: Check the result.

#By executing show eips topology-summary on the four devices, you can see that the EIPS ring status is round, and the topology content is consistent.

```

Master#show eips topology-summary
ring ID : 1
topo status : round
seq host-name mac type interface1 link interface2 link isBorder
-----
1 Transit3 0000.0000.008b transit gi0/2 UP gi0/1 UP NO
2 Transit2 0001.7a22.2224 transit gi0/2 UP gi0/1 UP YES
3 Transit1 0000.0010.0017 transit gi0/2 UP gi0/1 UP YES
4 Master 0001.7a54.5d71 master gi0/1 UP gi0/2 UP NO

```

```

Transit3#show eips topology-summary
ring ID : 1
topo status : round
seq host-name mac type interface1 link interface2 link isBorder
-----
1 Master 0001.7a54.5d71 master gi0/2 UP gi0/1 UP NO
2 Transit1 0000.0010.0017 transit gi0/1 UP gi0/2 UP YES
3 Transit2 0001.7a22.2224 transit gi0/1 UP gi0/2 UP YES
4 Transit3 0000.0000.008b transit gi0/1 UP gi0/2 UP NO

```

```

Transit1#show eips topology-summary
ring ID : 1
topo status : round
seq host-name mac type interface1 link interface2 link isBorder
-----
1 Transit2 0001.7a22.2224 transit gi0/1 UP gi0/2 UP YES
2 Transit3 0000.0000.008b transit gi0/1 UP gi0/2 UP NO
3 Master 0001.7a54.5d71 master gi0/2 UP gi0/1 UP NO
4 Transit1 0000.0010.0017 transit gi0/1 UP gi0/2 UP YES

```

Transit2#show eips topology-summary

ring ID : 1

topo status : round

seq	host-name	mac	type	interface1	link	interface2	link	isBorder
1	Transit3	0000.0000.008b	transit	gi0/1	UP	gi0/2	UP	NO
2	Master	0001.7a54.5d71	master	gi0/2	UP	gi0/1	UP	NO
3	Transit1	0000.0010.0017	transit	gi0/1	UP	gi0/2	UP	YES
4	Transit2	0001.7a22.2224	transit	gi0/1	UP	gi0/2	UP	YES

#By executing show eips topology on the four devices, you can see that the slave port gigabitethernet0/2 of the master node Master is blocked, and all other ports are unblocked.

Master#show eips topology

ring ID : 1

topo status : round

topo index 1 :

host name : Transit3

eips type : transit

eips status : COMPLETE

border : NO

base MAC : 0000.0000.008b

sys oid : 1.3.6.1.4.1.5651.1.102.146

interface1 : gi0/2

MAC : 0000.0000.008b

role : second

block-status : unblock

link-status : UP

interface2 : gi0/1

MAC : 0000.0000.008b

role : primary

block-status : unblock

link-status : UP

topo index 2 :

host name : Transit2

eips type : transit

eips status : COMPLETE

border : YES

base MAC : 0001.7a22.2224

sys oid : 1.3.6.1.4.1.5651.1.102.146

interface1 : gi0/2

```
MAC      : 0001.7a22.2224
role     : second
block-status : unblock
link-status : UP
interface2 : gi0/1
MAC      : 0001.7a22.2224
role     : primary
block-status : unblock
link-status : UP
topo index 3 :
host name : Transit1
eips type : transit
eips status : COMPLETE
border    : YES
base MAC  : 0000.0010.0017
sys oid   : 1.3.6.1.4.1.5651.1.102.140
interface1 : gi0/2
MAC      : 0000.0010.0017
role     : second
block-status : unblock
link-status : UP
interface2 : gi0/1
MAC      : 0000.0010.0017
role     : primary
block-status : unblock
link-status : UP
topo index 4 :
host name : Master
eips type : master
eips status : COMPLETE
border    : NO
base MAC  : 0001.7a54.5d71
sys oid   : 1.3.6.1.4.1.5651.1.102.145
interface1 : gi0/1
MAC      : 0001.7a54.5d71
role     : primary
block-status : unblock
link-status : UP
interface2 : gi0/2
MAC      : 0001.7a54.5d71
```

```
role      : second
block-status : block
link-status : UP
```

#When the link between transmission nodes Transit1 and Transit2 is disconnected, you can see through show eips topology that status of the ring turns to round, status of EIPS becomes FAULT, slave port gigabitethernet0/2 of the master node Master is unblocked, and Transit1 can communicate with Transit2 through the master node Master to ensure the communication between Transit1 and Transit2 is uninterrupted.

```
Master#show eips topology
ring ID      : 1
topo status  : not round
topo index 1 :
  host name   : Transit1
  eips type   : transit
  eips status : FAULT
  border      : YES
  base MAC    : 0000.0010.0017
  sys oid     : 1.3.6.1.4.1.5651.1.102.140
  interface1  : gi0/2
  MAC         : 0000.0010.0017
  role        : second
  block-status : block
  link-status : DOWN
  interface2  : gi0/1
  MAC         : 0000.0010.0017
  role        : primary
  block-status : unblock
  link-status : UP
topo index 2 :
  host name   : Master
  eips type   : master
  eips status : FAULT
  border      : NO
  base MAC    : 0001.7a54.5d71
  sys oid     : 1.3.6.1.4.1.5651.1.102.145
  interface1  : gi0/1
  MAC         : 0001.7a54.5d71
  role        : primary
  block-status : unblock
  link-status : UP
```

```
interface2 : gi0/2
MAC       : 0001.7a54.5d71
role      : second
block-status : unblock

link-status : UP
topo index 3 :
host name  : Transit3
eips type  : transit
eips status : FAULT
border     : NO
base MAC   : 0000.0000.008b
sys oid    : 1.3.6.1.4.1.5651.1.102.146
interface1 : gi0/2
MAC       : 0000.0000.008b
role      : second
block-status : unblock

link-status : UP
interface2 : gi0/1
MAC       : 0000.0000.008b
role      : primary
block-status : unblock

link-status : UP
topo index 4 :
host name  : Transit2
eips type  : transit
eips status : FAULT
border     : YES
base MAC   : 0001.7a22.2224
sys oid    : 1.3.6.1.4.1.5651.1.102.146
interface1 : gi0/2
MAC       : 0001.7a22.2224
role      : second
block-status : unblock

link-status : UP
interface2 : gi0/1
MAC       : 0001.7a22.2224
role      : primary
block-status : block

link-status : DOWN
```

### 101.3.2 Configure the Intersecting Rings in EIPS Hierarchy Segment Mode

#### Network Requirements

- There are six devices within the LAN, which make up two levels of intersecting rings. Protect the ring network by configuring EIPS hierarchy segment mode to block the slave port gigabitethernet0/2 of master node Master and the edge port gigabitethernet0/3 of edge node Transit1.
- When the link between the edge node Transit1 and the assistant edge node Transit2 is disconnected, it can cancel the spanning tree blocking state of the slave port gigabitethernet0/2 of the main ring's master node Master so that data switch and the communication in the main ring Ring1 are not affected.
- When the link between transmission nodes sTransit1 and sTransit2 is disconnected, it can cancel the spanning tree blocking state of the edge node Transit1's edge port gigabitethernet0/3 so that data switch and the communication in the first level of subring Ring2 are not affected.

#### Network Topology

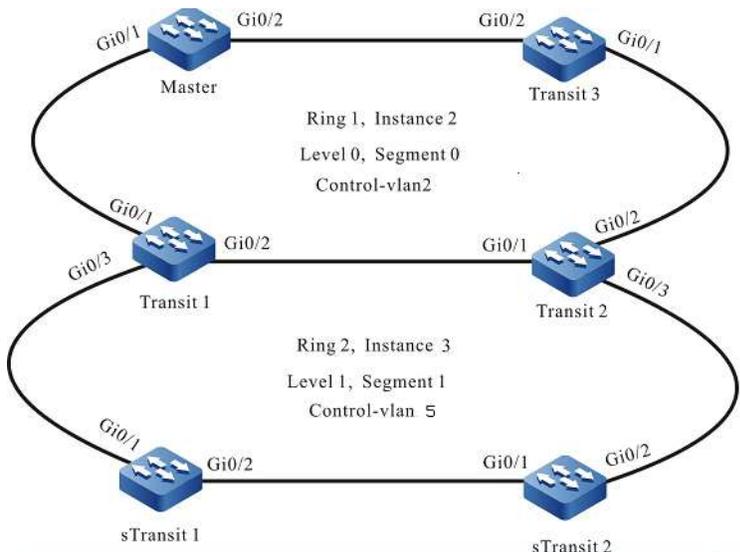


Figure 3 Network Topology for Configuring Intersecting Rings in EIPS Hierarchy Segment Mode

#### Configuration Steps

Step 1: Configure VLANs, and configure the link type of the ports.

#On Master, create VLAN2 and VLAN3, and configure the link type of ports gigabitethernet0/1~gigabitethernet0/2 as Trunk, permitting services of VLAN2 and VLAN3 to pass. Configure PVID as 1.

```

Master#configure terminal
Master(config)#vlan 2-3
Master(config)#interface gigabitethernet 0/1-0/2
Master(config-if-range)#switchport mode trunk
Master(config-if-range)#switchport trunk allowed vlan add 2-3
Master(config-if-range)#switchport trunk pvid vlan 1

```

#On Master, map VLAN3 to the spanning tree instance 2, and close spanning tree and storm suppression functions on ports gigabitethernet0/1~gigabitethernet0/2.

```

Master (config)#spanning-tree mst configuration
%Alert: Commands configured under the mode would not take effect immediately, you should active them explicitly!
Master (config-mst)#instance 2 vlan 3
Master (config-mst)#active configuration pending
Master(config-if-range)#exit
Master(config)#interface gigabitethernet 0/1-0/2
Master(config-if-range)#no spanning-tree enable
Master(config-if-range)#no storm-control multicast
Master(config-if-range)#no storm-control unicast
Master(config-if-range)#no storm-control broadcast
Master(config-if-range)#exit

```

#On the transmission node Transit1 of the main ring, create VLAN2-5, map VLAN3 to the spanning tree instance 2 and VLAN4 to the spanning tree instance 3, configure the link type of ports gigabitethernet0/1~gigabitethernet0/2 as Trunk to permit services of VLAN2-3 to pass and that of ports gigabitethernet0/2~gigabitethernet0/3 as Trunk to permit services of VLAN4-5 to pass, and configure PVID as 1. Close spanning tree and storm suppression functions on ports gigabitethernet0/1~gigabitethernet0/3. (Omitted)

#On the transmission node Transit2 of the main ring, create VLAN2-5, map VLAN3 to the spanning tree instance 2 and VLAN4 to the spanning tree instance 3, configure the link type of ports gigabitethernet0/1~gigabitethernet0/2 as Trunk to permit services of VLAN2-3 to pass and that of ports gigabitethernet0/2~gigabitethernet0/3 as Trunk to permit services of VLAN4-5 to pass, and configure PVID as 1. Close spanning tree and storm suppression functions on ports gigabitethernet0/1~gigabitethernet0/3. (Omitted)

#On the transmission node Transit3 of the main ring, create VLAN2 and VLAN3, map VLAN3 to the spanning tree instance 2, configure the link type of ports gigabitethernet0/1~gigabitethernet0/2 as Trunk, permitting services of VLAN2 and VLAN3 to pass, and configure PVID as 1. Close spanning tree and storm suppression functions on ports gigabitethernet0/1~gigabitethernet0/2. (Omitted)

#On the transmission node sTransit1 of the first level of subring, create VLAN4 and VLAN5, map VLAN4 to the spanning tree instance 3, configure the link type of ports gigabitethernet0/1~gigabitethernet0/2 as Trunk, permitting services of VLAN4 and VLAN5 to pass, and configure PVID as 1. Close spanning tree and storm suppression functions on ports gigabitethernet0/1~gigabitethernet0/2. (Omitted)

#On the transmission node Transit2 of the first level of subring, create VLAN4 and VLAN5, map VLAN4 to the spanning tree instance 3, configure the link type of ports gigabitethernet0/1~gigabitethernet0/2 as Trunk, permitting services of VLAN4 and VLAN5 to pass, and configure PVID as 1. Close spanning tree and storm suppression functions on ports gigabitethernet0/1~gigabitethernet0/2. (Omitted)

---

## Note

- VLAN5 is a control VLAN used to transmit EIPS protocol packets, and VLAN4 is a data VLAN used to forward services.
  - To use the EIPS function, you must map the EIPS data VLAN to corresponding spanning tree instance, and disable spanning tree and storm suppression functions on the port.
- 

Step 2: Configure the main ring Ring1.

#On the master node Master, create master node Ring1 in hierarchy segment mode, configure the level and segment number of EIPS ring as 0, instance of EIPS ring as 2, control VLAN as VLAN2, master port as gigabitethernet0/1 and slave port as gigabitethernet0/2, and enable EIPS.

```
Master(config)#eips ring 1 master segment
Master(config-eips)#control vlan 2
Master(config-eips)#level 0
Master(config-eips)#segment 0
Master(config-eips)#instance 2
Master(config-eips)#primary interface gigabitethernet 0/1
Master(config-eips)#secondary interface gigabitethernet 0/2
Master(config-eips)#eips start
Master(config-eips)#exit
```

#On the transmission node Transit1 of the main ring, create transmission node Ring1 in hierarchy segment mode, configure the level and segment number of EIPS ring as 0, instance of EIPS ring as 2, control VLAN as VLAN2, master port as gigabitethernet0/1 and slave port as gigabitethernet0/2, and enable EIPS. (Omitted)

#On the transmission node Transit2 of the main ring, create transmission node Ring1 in hierarchy segment mode, configure the level and segment number of EIPS ring as 0, instance of EIPS ring as 2, control VLAN as VLAN2, master port as gigabitethernet0/1 and slave port as gigabitethernet0/2, and enable EIPS. (Omitted)

#On the transmission node Transit3 of the main ring, create transmission node Ring1 in hierarchy segment mode, configure the level and segment number of EIPS ring as 0, instance of EIPS ring as 2, control VLAN as VLAN2, master port as gigabitethernet0/1 and slave port as gigabitethernet0/2, and enable EIPS. (Omitted)

Step 3: Configure the first-level subring Ring2.

#On the edge node of the first-level subring (transmission node of the main ring), create edge node Ring2 of hierarchy segment mode on Transit1, configure the level and segment number of EIPS ring as 1, instance of EIPS ring as 3, control VLAN as VLAN5, edge port as gigabitethernet0/3 and Ring1 as its associated transmission node, and enable EIPS.

```
Transit1(config)#eips ring 2 edge segment
Transit1(config-eips)#control vlan 5
Transit1(config-eips)#level 1
Transit1(config-eips)#segment 1
Transit1(config-eips)#instance 3
Transit1(config-eips)#transit ring 1
Transit1(config-eips)#edge interface gigabitethernet0/3
Transit1(config-eips)#eips start
Transit1(config-eips)#exit
```

#On the assistant edge node of the first-level subring (transmission node of the main ring), create assistant edge node Ring2 of hierarchy segment mode on Transit2, configure the level and segment number of EIPS ring as 1, instance of EIPS ring as 3, control VLAN as VLAN5, edge port as gigabitethernet0/3 and Ring1 as its associated transmission node, and enable EIPS.

```
Transit2(config)#eips ring 2 assistant segment
Transit2(config-eips)#control vlan 5
Transit2(config-eips)#level 1
Transit2(config-eips)#segment 1
Transit2(config-eips)#instance 3
Transit2(config-eips)#transit ring 1
Transit2(config-eips)#edge interface gigabitethernet0/3
Transit2(config-eips)#eips start
Transit2(config-eips)#exit
```

#On the transmission node sTransit1 of the first-level subring, create transmission node Ring2 in hierarchy segment mode, configure the level and segment number of EIPS ring as 1, instance of EIPS ring as 3, control VLAN as VLAN5, master port as gigabitethernet0/1 and slave port as gigabitethernet0/2, and enable EIPS.

```
sTransit1(config)#eips ring 2 transit segment
sTransit1(config-eips)#control vlan 5
sTransit1(config-eips)#level 1
sTransit1(config-eips)#segment 1
sTransit1(config-eips)#instance 3
sTransit1(config-eips)#primary interface gigabitethernet 0/1
sTransit1(config-eips)#secondary interface gigabitethernet 0/2
sTransit1(config-eips)#eips start
sTransit1(config-eips)#exit
```

#On the transmission node Transit2 of the first-level subring, create transmission node Ring2 in hierarchy segment mode, configure the level and segment number of EIPS ring as 1, instance of EIPS ring as 3, control VLAN as VLAN5, master port as gigabitethernet0/1 and slave port as gigabitethernet0/2, and enable EIPS.

```
sTransit2(config)#eips ring 2 transit segment
sTransit2(config-eips)#control vlan 5
sTransit2(config-eips)#level 1
sTransit2(config-eips)#segment 1
sTransit2(config-eips)#instance 3
sTransit2(config-eips)#primary interface gigabitethernet 0/1
sTransit2(config-eips)#secondary interface gigabitethernet 0/2
sTransit2(config-eips)#eips start
sTransit2(config-eips)#exit
```

Step 4: Check the result.

#By executing show eips topology-summary on edge node and assistant edge node, you can see that the status of both EIPS main ring and subring is round, and the topology content is consistent.

```
Transit1#show eips topology-summary
```

```
ring ID : 1
```

```
topo status : round
```

seq	host-name	mac	type	interface1	link	interface2	link	isBorder
1	Transit2	0001.7a22.2224	transit	gi0/1	UP	gi0/2	UP	YES
2	Transit3	0000.0000.008b	transit	gi0/1	UP	gi0/2	UP	NO
3	Master	0014.0000.1202	master	gi0/2	UP	gi0/1	UP	NO
4	Transit1	0001.7a54.5d71	transit	gi0/1	UP	gi0/2	UP	YES

```
ring ID : 2
```

```
topo status : round
```

seq	host-name	mac	type	interface1	link	interface2	link	isBorder
1	Transit2	0001.7a22.2224	assistant	----	----	gi0/3	UP	NO
2	sTransit2	2012.1209.1728	transit	gi0/2	UP	gi0/1	UP	NO
3	sTransit1	0000.0010.0017	transit	gi0/2	UP	gi0/1	UP	NO
4	Transit1	0001.7a54.5d71	edge	gi0/3	UP	----	----	NO

```
Transit2#show eips topology-summary
```

```
ring ID : 1
```

```
topo status : round
```

seq	host-name	mac	type	interface1	link	interface2	link	isBorder
1	Transit3	0000.0000.008b	transit	gi0/1	UP	gi0/2	UP	NO
2	Master	0014.0000.1202	master	gi0/2	UP	gi0/1	UP	NO
3	Transit1	0001.7a54.5d71	transit	gi0/1	UP	gi0/2	UP	YES
4	Transit2	0001.7a22.2224	transit	gi0/1	UP	gi0/2	UP	YES

ring ID : 2

topo status : round

seq	host-name	mac	type	interface1	link	interface2	link	isBorder
1	Transit1	0001.7a54.5d71	edge	---	---	gi0/3	UP	NO
2	sTransit1	0000.0010.0017	transit	gi0/1	UP	gi0/2	UP	NO
3	sTransit2	2012.1209.1728	transit	gi0/1	UP	gi0/2	UP	NO
4	Transit2	0001.7a22.2224	assistant	gi0/3	UP	---	---	NO

#By executing show eips topology on the edge node, you can see that the slave port gigabitethernet0/2 of the master node Master and the edge port gigabitethernet0/3 of the edge node Transit1 are blocked, and all other ports are unblocked; the EIPS status of main ring and subring is COMPLETE.

```

Transit1#show eips topology
ring ID : 1
topo status : round
topo index 1 :
  host name : Transit2
  eips type : transit
  eips status : COMPLETE
  border : YES
  base MAC : 0001.7a22.2224
  sys oid : 1.3.6.1.4.1.5651.1.0.0
  interface1 : gi0/1
  MAC : 0001.7a22.2224
  role : primary
  block-status : unblock
  link-status : UP
  interface2 : gi0/2
  MAC : 0001.7a22.2224
  role : second
  block-status : unblock
  link-status : UP
topo index 2 :

```

```
host name      : Transit3
eips type     : transit
eips status   : COMPLETE
border        : NO
base MAC      : 0000.0000.008b
sys oid       : 1.3.6.1.4.1.5651.1.102.146
interface1    : gi0/1
MAC           : 0000.0000.008b
role          : primary
block-status  : unblock
link-status   : UP
interface2    : gi0/2
MAC           : 0000.0000.008b
role          : second
block-status  : unblock
link-status   : UP
topo index 3  :
host name     : Master
eips type     : master
eips status   : COMPLETE
border        : NO
base MAC      : 0014.0000.1202
sys oid       : 1.3.6.1.4.1.5651.1.102.127
interface1    : gi0/2
MAC           : 0014.0000.1202
role          : second
block-status  : block
link-status   : UP
interface2    : gi0/1
MAC           : 0014.0000.1202
role          : primary
block-status  : unblock
link-status   : UP
topo index 4  :
host name     : Transit1
eips type     : transit
eips status   : COMPLETE
border        : YES
base MAC      : 0001.7a54.5d71
sys oid       : 1.3.6.1.4.1.5651.1.102.145
```

interface1 : gi0/1  
MAC : 0001.7a54.5d71  
role : primary  
block-status : unblock  
link-status : UP  
interface2 : gi0/2  
MAC : 0001.7a54.5d71  
role : second  
block-status : unblock  
link-status : UP

ring ID : 2

topo status : round

topo index 1 :

host name : Transit2  
eips type : assistant  
eips status : COMPLETE  
border : NO  
base MAC : 0001.7a22.2224  
sys oid : 1.3.6.1.4.1.5651.1.0.0  
interface2 : gi0/3  
MAC : 0001.7a22.2224  
role : edge  
block-status : unblock  
link-status : UP

topo index 2 :

host name : sTransit2  
eips type : transit  
eips status : COMPLETE  
border : NO  
base MAC : 2012.1209.1728  
sys oid : 1.3.6.1.4.1.5651.1.102.126  
interface1 : gi0/2  
MAC : 2012.1209.1728  
role : second  
block-status : unblock  
link-status : UP  
interface2 : gi0/1  
MAC : 2012.1209.1728  
role : primary

```

    block-status : unblock
    link-status  : UP
topo index 3 :
    host name    : sTransit1
    eips type    : transit
    eips status  : COMPLETE
    border      : NO
    base MAC    : 0000.0010.0017
    sys oid     : 1.3.6.1.4.1.5651.1.102.140
    interface1  : gi0/2
    MAC         : 0000.0010.0017
    role        : second
    block-status : unblock
    link-status  : UP
    interface2  : gi0/1
    MAC         : 0000.0010.0017
    role        : primary
    block-status : unblock
    link-status  : UP
topo index 4 :
    host name    : Transit1
    eips type    : edge
    eips status  : COMPLETE
    border      : NO
    base MAC    : 0001.7a54.5d71
    sys oid     : 1.3.6.1.4.1.5651.1.102.145
    interface1  : gi0/3
    MAC         : 0001.7a54.5d71
    role        : edge
    block-status : block
    link-status  : UP

```

#When the link between edge node Transit1 and assistant edge node Transit2 is disconnected, you can see on the edge node with show eips topology that the status of main ring Ring1 is not round, status of EIPS becomes FAULT, slave port gigabitethernet0/2 of the master node Master is unblocked, and Transit1 can communicate with Transit2 through the master node Master to ensure the communication between Transit1 and Transit2 is uninterrupted; the status of subring Ring2 is still round, the EIPS status is COMPLETE, and the edge port gigabitethernet0/3 of edge node Transit1 is blocked.

```

Transit1#show eips topology ring 1
ring ID   : 1

```

topo status : not round

topo index 1 :

host name : Transit2  
eips type : transit  
eips status : FAULT  
border : YES  
base MAC : 0001.7a22.2224  
sys oid : 1.3.6.1.4.1.5651.1.0.0  
interface1 : gi0/1  
MAC : 0001.7a22.2224  
role : primary  
block-status : block  
link-status : DOWN  
interface2 : gi0/2  
MAC : 0001.7a22.2224  
role : second  
block-status : unblock  
link-status : UP

topo index 2 :

host name : Transit3  
eips type : transit  
eips status : FAULT  
border : NO  
base MAC : 0000.0000.008b  
sys oid : 1.3.6.1.4.1.5651.1.102.146  
interface1 : gi0/1  
MAC : 0000.0000.008b  
role : primary  
block-status : unblock  
link-status : UP  
interface2 : gi0/2  
MAC : 0000.0000.008b  
role : second  
block-status : unblock  
link-status : UP

topo index 3 :

host name : Master  
eips type : master  
eips status : FAULT  
border : NO

```
base MAC      : 0014.0000.1202
sys oid       : 1.3.6.1.4.1.5651.1.102.127
interface1    : gi0/2
MAC           : 0014.0000.1202
role          : second
block-status  : unblock
link-status   : UP
interface2    : gi0/1
MAC           : 0014.0000.1202
role          : primary
block-status  : unblock
link-status   : UP
topo index 4  :
host name     : Transit1
eips type     : transit
eips status   : FAULT
border        : YES
base MAC      : 0001.7a54.5d71
sys oid       : 1.3.6.1.4.1.5651.1.102.145
interface1    : gi0/1
MAC           : 0001.7a54.5d71
role          : primary
block-status  : unblock
link-status   : UP
interface2    : gi0/2
MAC           : 0001.7a54.5d71
role          : second
block-status  : block
link-status   : DOWN
```

Transit1#show eips topology ring 2

```
ring ID      : 2
topo status  : round
topo index 1 :
host name    : Transit2
eips type    : assistant
eips status  : COMPLETE
border       : NO
base MAC     : 0001.7a22.2224
sys oid      : 1.3.6.1.4.1.5651.1.0.0
```

```
interface2 : gi0/3
MAC : 0001.7a22.2224
role : edge
block-status : unblock
link-status : UP
topo index 2 :
host name : sTransit2
eips type : transit
eips status : COMPLETE
border : NO
base MAC : 2012.1209.1728
sys oid : 1.3.6.1.4.1.5651.1.102.126
interface1 : gi0/2
MAC : 2012.1209.1728
role : second
block-status : unblock
link-status : UP
interface2 : gi0/1
MAC : 2012.1209.1728
role : primary
block-status : unblock
link-status : UP
topo index 3 :
host name : sTransit1
eips type : transit
eips status : COMPLETE
border : NO
base MAC : 0000.0010.0017
sys oid : 1.3.6.1.4.1.5651.1.102.140
interface1 : gi0/2
MAC : 0000.0010.0017
role : second
block-status : unblock
link-status : UP
interface2 : gi0/1
MAC : 0000.0010.0017
role : primary
block-status : unblock
link-status : UP
topo index 4 :
```

```

host name      : Transit1
eips type     : edge
eips status   : COMPLETE
border        : NO
base MAC      : 0001.7a54.5d71
sys oid       : 1.3.6.1.4.1.5651.1.102.145
interface1    : gi0/3
MAC           : 0001.7a54.5d71
role          : edge
block-status  : block
link-status   : UP

```

#When only the link between transmission nodes sTransit1 and sTransit2 is disconnected, you can see on the edge node and assistant edge node with show eips topology that the status of subring Ring2 is not round, status of EIPS becomes FAULT, edge port gigabitEthernet0/3 of the edge node Transit1 is unblocked, and sTransit1 can communicate with sTransit2 through edge node Transit1 to ensure the communication between sTransit1 and sTransit2 is uninterrupted; the status of main ring Ring1 is still round, the EIPS status is COMPLETE, and the slave port gigabitEthernet0/2 of master node Master is blocked.

```

Transit1#show eips topology ring 2
ring ID      : 2
topo status  : not round
topo index 1 :
  host name   : sTransit1
  eips type   : transit
  eips status : FAULT
  border      : NO
  base MAC    : 0000.0010.0017
  sys oid     : 1.3.6.1.4.1.5651.1.102.140
  interface1  : gi0/2
  MAC        : 0000.0010.0017
  role        : second
  block-status : block
  link-status : DOWN
  interface2  : gi0/1
  MAC        : 0000.0010.0017
  role        : primary
  block-status : unblock
  link-status : UP
topo index 2 :
  host name   : Transit1

```

eips type : edge  
eips status : FAULT  
border : NO  
base MAC : 0001.7a54.5d71  
sys oid : 1.3.6.1.4.1.5651.1.102.145  
interface1 : gi0/3  
MAC : 0001.7a54.5d71  
role : edge  
block-status : unblock  
link-status : UP

Transit2#show eips topology ring 2

ring ID : 2

topo status : not round

topo index 1 :

host name : sTransit2  
eips type : transit  
eips status : FAULT  
border : NO  
base MAC : 2012.1209.1728  
sys oid : 1.3.6.1.4.1.5651.1.102.126  
interface1 : gi0/1  
MAC : 2012.1209.1728  
role : primary  
block-status : block  
link-status : DOWN  
interface2 : gi0/2  
MAC : 2012.1209.1728  
role : second  
block-status : unblock  
link-status : UP

topo index 2 :

host name : Transit2  
eips type : assistant  
eips status : FAULT  
border : NO  
base MAC : 0001.7a22.2224  
sys oid : 1.3.6.1.4.1.5651.1.0.0  
interface1 : gi0/3  
MAC : 0001.7a22.2224  
role : edge

```
    block-status : unblock
    link-status  : UP
Transit1#show eips topology ring 1
ring ID   : 1
topo status : round
topo index 1 :
    host name   : Transit2
    eips type   : transit
    eips status : COMPLETE
    border     : YES
    base MAC    : 0001.7a22.2224
    sys oid    : 1.3.6.1.4.1.5651.1.0.0
    interface1 : gi0/1
    MAC        : 0001.7a22.2224
    role       : primary
    block-status : unblock
    link-status  : UP
    interface2 : gi0/2
    MAC        : 0001.7a22.2224
    role       : second
    block-status : unblock
    link-status  : UP
topo index 2 :
    host name   : Transit3
    eips type   : transit
    eips status : COMPLETE
    border     : NO
    base MAC    : 0000.0000.008b
    sys oid    : 1.3.6.1.4.1.5651.1.102.146
    interface1 : gi0/1
    MAC        : 0000.0000.008b
    role       : primary
    block-status : unblock
    link-status  : UP
    interface2 : gi0/2
    MAC        : 0000.0000.008b
    role       : second
    block-status : unblock
    link-status  : UP
topo index 3 :
```

```
host name      : Master
eips type     : master
eips status   : COMPLETE
border        : NO
base MAC      : 0014.0000.1202
sys oid       : 1.3.6.1.4.1.5651.1.102.127
interface1    : gi0/2
MAC           : 0014.0000.1202
role          : second
block-status  : block
link-status   : UP
interface2    : gi0/1
MAC           : 0014.0000.1202
role          : primary
block-status  : unblock
link-status   : UP
topo index 4  :
host name     : Transit1
eips type     : transit
eips status   : COMPLETE
border        : YES
base MAC      : 0001.7a54.5d71
sys oid       : 1.3.6.1.4.1.5651.1.102.145
interface1    : gi0/1
MAC           : 0001.7a54.5d71
role          : primary
block-status  : unblock
link-status   : UP
interface2    : gi0/2
MAC           : 0001.7a54.5d71
role          : second
block-status  : unblock
link-status   : UP
```

### 101.3.3 Configure the Intersecting Rings in EIPS Subring Mode

#### Network Requirements

- There are six devices within the LAN, which make up two levels of intersecting rings. Protect the ring network by configuring EIPS subring mode to block the slave port

gigabitethernet0/2 of main ring's master node Master and the slave port gigabitethernet0/2 of subring's master node sMaster.

- When the link between the main ring's transmission nodes Transit1 and Transit2 is disconnected, it can cancel the spanning tree blocking state of the slave port gigabitethernet0/2 of the main ring's master node Master so that data switch and the communication in the main ring Ring1 are not affected.
- When the link between subring's transmission node sTransit1 and main ring's transmission node Transit2 is disconnected, it can cancel the spanning tree blocking state of the slave port of subring's master node of sMaster gigabitethernet0/2 so that data switch and the communication in subring Ring2 are not affected.

### Network Topology

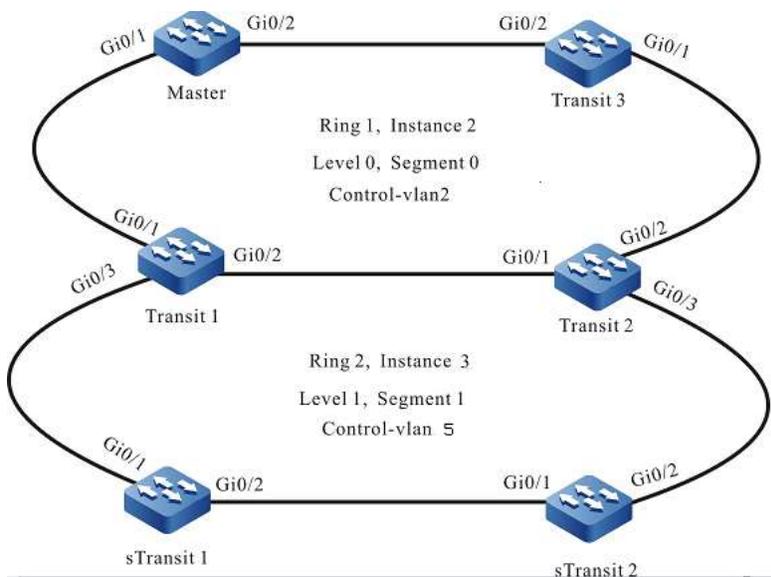


Figure 4 Network Topology for Configuring Intersecting Rings in EIPS Subring Mode

### Configuration Steps

Step 1: Configure VLANs, and configure the link type of the ports.

#On Master, create VLAN2~VLAN3, and configure the link type of ports gigabitethernet0/1~gigabitethernet0/2 as Trunk, permitting services of VLAN2-VLAN3 to pass. Configure PVID as 1.

```

Master#configure terminal
Master(config)#vlan 2-4
Master(config)#interface gigabitethernet 0/1-0/2
Master(config-if-range)#switchport mode trunk
Master(config-if-range)#switchport trunk allowed vlan add 2-3
Master(config-if-range)#switchport trunk pvid vlan 1

```

#On Master, map VLAN3 to the spanning tree instance 2, and close spanning tree and storm suppression functions on ports gigabitethernet0/1~gigabitethernet0/2.

```
Master (config)#spanning-tree mst configuration
%Alert: Commands configured under the mode would not take effect immediately, you should active them explicitly!
Master (config-mst)#instance 2 vlan 3
Master (config-mst)#active configuration pending
Master(config-if-range)#exit
Master(config)#interface gigabitethernet 0/1-0/2
Master(config-if-range)#no spanning-tree enable
Master(config-if-range)#no storm-control multicast
Master(config-if-range)#no storm-control unicast
Master(config-if-range)#no storm-control broadcast
Master(config-if-range)#exit
```

#On the transmission node Transit1 of the main ring, create VLAN2-5, map VLAN3 to the spanning tree instance 2 and VLAN4 to the spanning tree instance 3, configure the link type of ports gigabitethernet0/1~gigabitethernet0/2 as Trunk to permit services of VLAN2-3 to pass and that of ports gigabitethernet0/2~gigabitethernet0/3 as Trunk to permit services of VLAN4-5 to pass, and configure PVID as 1. Close spanning tree and storm suppression functions on ports gigabitethernet0/1~gigabitethernet0/3. (Omitted)

#On the transmission node Transit2 of the main ring, create VLAN2-5, map VLAN3 to the spanning tree instance 2 and VLAN4 to the spanning tree instance 3, configure the link type of ports gigabitethernet0/1~gigabitethernet0/2 as Trunk to permit services of VLAN2-3 to pass and that of ports gigabitethernet0/2~gigabitethernet0/3 as Trunk to permit services of VLAN4-5 to pass, and configure PVID as 1. Close spanning tree and storm suppression functions on ports gigabitethernet0/1~gigabitethernet0/3. (Omitted)

#On the transmission node Transit3 of the main ring, create VLAN2 and VLAN3, map VLAN3 to the spanning tree instance 2, configure the link type of ports gigabitethernet0/1~gigabitethernet0/2 as Trunk, permitting services of VLAN2 and VLAN3 to pass, and configure PVID as 1. Close spanning tree and storm suppression functions on ports gigabitethernet0/1~gigabitethernet0/2. (Omitted)

#On the transmission node sTransit1 of the first level of subring, create VLAN4 and VLAN5, map VLAN4 to the spanning tree instance 3, configure the link type of ports gigabitethernet0/1~gigabitethernet0/2 as Trunk, permitting services of VLAN4 and VLAN5 to pass, and configure PVID as 1. Close spanning tree and storm suppression functions on ports gigabitethernet0/1~gigabitethernet0/2. (Omitted)

#On the transmission node Transit2 of the first level of subring, create VLAN4 and VLAN5, map VLAN4 to the spanning tree instance 3, configure the link type of ports gigabitethernet0/1~gigabitethernet0/2 as Trunk, permitting services of VLAN4 and VLAN5 to pass, and configure PVID as 1. Close spanning tree and storm suppression functions on ports gigabitethernet0/1~gigabitethernet0/2. (Omitted)

---

 **Note**

- VLAN2 is a control VLAN of main ring and VLAN5 is a control VLAN of subring, used to transmit EIPS protocol packets; VLAN3-4 are data VLANs used to forward services.
  - To use the EIPS function, you must map the EIPS data VLAN to corresponding spanning tree instance, and disable spanning tree and storm suppression functions on the port.
- 

Step 2: Configure the main ring Ring1.

#On the master node Master, create master node Ring1 in subring mode, configure the level of EIPS ring as 0, domain of EIPS ring as 1, instance of EIPS ring as 2, control VLAN as VLAN2, master port as gigabitethernet0/1 and slave port as gigabitethernet0/2, and enable EIPS.

```
Master(config)#eips ring 1 master
Master(config-eips)#control vlan 2
Master(config-eips)#level 0
Master(config-eips)#domain id 1
Master(config-eips)#instance 2
Master(config-eips)#primary interface gigabitethernet 0/1
Master(config-eips)#secondary interface gigabitethernet 0/2
Master(config-eips)#eips start
Master(config-eips)#exit
```

#On the transmission node Transit1 of the main ring, create transmission node Ring1 in subring mode, configure the level of EIPS ring as 0, domain of EIPS ring as 1, instance of EIPS ring as 2, control VLAN as VLAN2, master port as gigabitethernet0/1 and slave port as gigabitethernet0/2, and enable EIPS.

```
Transit1(config)#eips ring 1 transit
Transit1(config-eips)#instance 2
Transit1(config-eips)#control vlan 2
Transit1(config-eips)#domain id 1
Transit1(config-eips)#level 0
Transit1(config-eips)#primary interface gigabitethernet0/1
Transit1(config-eips)#secondary interface gigabitethernet0/2
Transit1(config-eips)#eips start
Transit1(config-eips)#exit
```

#On the transmission node Transit2 of the main ring, create transmission node Ring1 in subring mode, configure the level of EIPS ring as 0, domain of EIPS ring as 1, instance of EIPS ring as 2, control VLAN as VLAN2, master port as gigabitethernet0/1 and slave port as gigabitethernet0/2, and enable EIPS.

```
Transit2(config)#eips ring 1 transit
Transit2(config-eips)#instance 2
```

```

Transit2(config-eips)#domain id 1
Transit2(config-eips)#control vlan 2
Transit2(config-eips)#level 0
Transit2(config-eips)#primary interface gigabitethernet0/1
Transit2(config-eips)#secondary interface gigabitethernet0/2
Transit2(config-eips)#eips start
Transit2(config-eips)#exit

```

#On the transmission node Transit3 of the main ring, create transmission node Ring1 in subring mode, configure the level of EIPS ring as 0, domain of EIPS ring as 1, instance of EIPS ring as 2, control VLAN as VLAN2, master port as gigabitethernet0/1 and slave port as gigabitethernet0/2, and enable EIPS.

```

Transit3(config)#eips ring 1 transit
Transit3(config-eips)#control vlan 2
Transit3(config-eips)#level 0
Transit3(config-eips)#domain id 1
Transit3(config-eips)#instance 2
Transit3(config-eips)#primary interface gigabitethernet 0/1
Transit3(config-eips)#secondary interface gigabitethernet 0/2
Transit3(config-eips)#eips start
Transit3(config-eips)#exit

```

### Step 3: Configure the subring Ring2.

#On the edge node of the subring (transmission node of the main ring), create edge node Ring2 of subring mode on Transit1, configure the level and domain of EIPS ring as 1, instance of EIPS ring as 3, control VLAN as VLAN5, edge port as gigabitethernet0/3 and Ring1 as its associated transmission node, and enable EIPS.

```

Transit1(config)#eips ring 2 edge
Transit1(config-eips)#control vlan 5
Transit1(config-eips)#level 1
Transit1(config-eips)#domain id 1
Transit1(config-eips)#instance 3
Transit1(config-eips)#transit ring 1
Transit1(config-eips)#edge interface gigabitethernet0/3
Transit1(config-eips)#eips start
Transit1(config-eips)#exit

```

#On the assistant edge node of the subring (transmission node of the main ring), create assistant edge node Ring2 of subring mode on Transit2, configure the level and domain of EIPS ring as 1, instance of EIPS ring as 3, control VLAN as VLAN5, edge port as gigabitethernet0/3 and Ring1 as its associated transmission node, and enable EIPS.

```

Transit2(config)#eips ring 2 assistant

```

```
Transit2(config-eips)#control vlan 5
Transit2(config-eips)#level 1
Transit2(config-eips)#domain id 1
Transit2(config-eips)#instance 3
Transit2(config-eips)#transit ring 1
Transit2(config-eips)#edge interface gigabitethernet0/3
Transit2(config-eips)#eips start
Transit2(config-eips)#exit
```

#On the master node sMaster of the subring, create master node Ring2 in subring mode, configure the level and domain of EIPS ring as 1, instance of EIPS ring as 3, control VLAN as VLAN5, master port as gigabitethernet0/1 and slave port as gigabitethernet0/2, and enable EIPS.

```
sMaster(config)#eips ring 2 master
sMaster(config-eips)#level 1
sMaster(config-eips)#domain id 1
sMaster(config-eips)#instance 3
sMaster(config-eips)#control vlan 5
sMaster(config-eips)#primary interface gigabitethernet 0/1
sMaster(config-eips)#secondary interface gigabitethernet 0/2
sMaster(config-eips)#eips start
sMaster(config-eips)#exit
```

#On the transmission node sTransit1 of the subring, create transmission node Ring2 in subring mode, configure the level and domain of EIPS ring as 1, instance of EIPS ring as 3, control VLAN as VLAN5, master port as gigabitethernet0/1 and slave port as gigabitethernet0/2, and enable EIPS.

```
sTransit1(config)#eips ring 2 transit
sTransit1(config-eips)#control vlan 5
sTransit1(config-eips)#level 1
sTransit1(config-eips)#domain id 1
sTransit1(config-eips)#instance 3
sTransit1(config-eips)#primary interface gigabitethernet 0/1
sTransit1(config-eips)#secondary interface gigabitethernet 0/2
sTransit1(config-eips)#eips start
sTransit1(config-eips)#exit
```

Step  
4:

Check the result.

#By executing show eips topology-summary on edge node and assistant edge node, you can see that the status of both EIPS main ring and subring is round, and the topology content is consistent.

```
Transit1#show eips topology-summary
```

ring ID : 1

topo status : round

seq	host-name	mac	type	interface1	link	interface2	link	isBorder
1	Transit2	0001.7a22.2224	transit	gi0/1	UP	gi0/2	UP	YES
2	Transit3	0000.0000.008b	transit	gi0/1	UP	gi0/2	UP	NO
3	Master	0014.0000.1202	master	gi0/2	UP	gi0/1	UP	NO
4	Transit1	0001.7a54.5d71	transit	gi0/1	UP	gi0/2	UP	YES

ring ID : 2

topo status : round

seq	host-name	mac	type	interface1	link	interface2	link	isBorder
1	Transit2	0001.7a22.2224	assistant	---	---	gi0/3	UP	NO
2	sTransit1	2012.1209.1728	transit	gi0/2	UP	gi0/1	UP	NO
3	sMaster	0000.0010.0017	master	gi0/2	UP	gi0/1	UP	NO
4	Transit1	0001.7a54.5d71	edge	gi0/3	UP	---	---	NO

Transit2#show eips topology-summary

ring ID : 1

topo status : round

seq	host-name	mac	type	interface1	link	interface2	link	isBorder
1	Transit3	0000.0000.008b	transit	gi0/1	UP	gi0/2	UP	NO
2	Master	0014.0000.1202	master	gi0/2	UP	gi0/1	UP	NO
3	Transit1	0001.7a54.5d71	transit	gi0/1	UP	gi0/2	UP	YES
4	Transit2	0001.7a22.2224	transit	gi0/1	UP	gi0/2	UP	YES

ring ID : 2

topo status : round

seq	host-name	mac	type	interface1	link	interface2	link	isBorder
1	Transit1	0001.7a54.5d71	edge	---	---	gi0/3	UP	NO
2	sMaster	0000.0010.0017	master	gi0/1	UP	gi0/2	UP	NO
3	sTransit1	2012.1209.1728	transit	gi0/1	UP	gi0/2	UP	NO
4	Transit2	0001.7a22.2224	assistant	gi0/3	UP	---	---	NO

#By executing show eips topology on the edge node, you can see that the slave port gigabitethernet0/2 of the main ring's master node Master and the slave port gigabitethernet0/2 of the subring's master node sMaster are blocked, and all other ports are unblocked; the EIPS status of main ring's master node Master and subring's master node sMaster is COMPLETE, and that of all other nodes is LINK-UP.

```
Transit1#show eips topology
ring ID      : 1
topo status  : round
topo index 1 :
  host name   : Transit2
  eips type   : transit
  eips status : LINK-UP
  border      : YES
  base MAC    : 0001.7a22.2224
  sys oid     : 1.3.6.1.4.1.5651.1.0.0
  interface1  : gi0/1
  MAC         : 0001.7a22.2224
  role        : primary
  block-status : unblock
  link-status  : UP
  interface2  : gi0/2
  MAC         : 0001.7a22.2224
  role        : second
  block-status : unblock
  link-status  : UP
topo index 2 :
  host name   : Transit3
  eips type   : transit
  eips status : LINK-UP
  border      : NO
  base MAC    : 0000.0000.008b
  sys oid     : 1.3.6.1.4.1.5651.1.102.146
  interface1  : gi0/1
  MAC         : 0000.0000.008b
  role        : primary
  block-status : unblock
  link-status  : UP
  interface2  : gi0/2
  MAC         : 0000.0000.008b
  role        : second
  block-status : unblock
  link-status  : UP
topo index 3 :
  host name   : Master
  eips type   : master
```

```
eips status : COMPLETE

border      : NO

base MAC    : 0014.0000.1202

sys oid     : 1.3.6.1.4.1.5651.1.102.127

interface1  : gi0/2

MAC         : 0014.0000.1202

role        : second

block-status : block

link-status : UP

interface2  : gi0/1

MAC         : 0014.0000.1202

role        : primary

block-status : unblock

link-status : UP

topo index 4 :

host name   : Transit1

eips type   : transit

eips status : LINK-UP

border      : YES

base MAC    : 0001.7a54.5d71

sys oid     : 1.3.6.1.4.1.5651.1.102.145

interface1  : gi0/1

MAC         : 0001.7a54.5d71

role        : primary

block-status : unblock

link-status : UP

interface2  : gi0/2

MAC         : 0001.7a54.5d71

role        : second

block-status : unblock

link-status : UP

ring ID     : 2

topo status : round

topo index 1 :

host name   : Transit2

eips type   : assistant

eips status : LINK-UP

border      : NO

base MAC    : 0001.7a22.2224
```

```
sys oid      : 1.3.6.1.4.1.5651.1.0.0
interface2   : gi0/3
MAC          : 0001.7a22.2224
role         : edge
block-status : unblock
link-status  : UP
topo index 2 :
host name    : sTransit1
eips type    : transit
eips status  : LINK-UP
border       : NO
base MAC     : 2012.1209.1728
sys oid      : 1.3.6.1.4.1.5651.1.102.126
interface1   : gi0/2
MAC          : 2012.1209.1728
role         : second
block-status : unblock
link-status  : UP
interface2   : gi0/1
MAC          : 2012.1209.1728
role         : primary
block-status : unblock
link-status  : UP
topo index 3 :
host name    : sMaster
eips type    : master
eips status  : COMPLETE
border       : NO
base MAC     : 0000.0010.0017
sys oid      : 1.3.6.1.4.1.5651.1.102.140
interface1   : gi0/2
MAC          : 0000.0010.0017
role         : second
block-status : block
link-status  : UP
interface2   : gi0/1
MAC          : 0000.0010.0017
role         : primary
block-status : unblock
link-status  : UP
```

```

topo index 4 :
  host name    : Transit1
  eips type    : edge
  eips status  : LINK-UP
  border       : NO
  base MAC     : 0001.7a54.5d71
  sys oid     : 1.3.6.1.4.1.5651.1.102.145
  interface1   : gi0/3
  MAC         : 0001.7a54.5d71
  role         : edge
  block-status : unblock
  link-status  : UP

```

#When the link between transmission nodes of the main ring Transit1 and Transit2 is disconnected, you can see on the edge node with show eips topology that the status of main ring Ring1 is not round, EIPS status of Transit1 and Transit2 becomes LINK-DOWN, EIPS status of the main ring's master node Master becomes FAULT, slave port gigabitethernet0/2 of the main ring's master node Master is unblocked, and Transit1 can communicate with Transit2 through the main ring's master node Master to ensure the communication between Transit1 and Transit2 is uninterrupted; the status of subring Ring2 is still round, the EIPS status of subring's master node sMaster is still COMPLETE, and the slave port gigabitethernet0/2 of subring's master node sMaster is still blocked.

```

Transit1#show eips topology ring 1
ring ID      : 1
topo status  : not round
topo index 1 :
  host name    : Transit2
  eips type    : transit
  eips status  : LINK-DOWN
  border       : YES
  base MAC     : 0001.7a22.2224
  sys oid     : 1.3.6.1.4.1.5651.1.0.0
  interface1   : gi0/1
  MAC         : 0001.7a22.2224
  role         : primary
  block-status : block
  link-status  : DOWN
  interface2   : gi0/2
  MAC         : 0001.7a22.2224
  role         : second
  block-status : unblock
  link-status  : UP

```

topo index 2 :  
host name : Transit3  
eips type : transit  
eips status : LINK-UP  
border : NO  
base MAC : 0000.0000.008b  
sys oid : 1.3.6.1.4.1.5651.1.102.146  
interface1 : gi0/1  
MAC : 0000.0000.008b  
role : primary  
block-status : unblock  
link-status : UP  
interface2 : gi0/2  
MAC : 0000.0000.008b  
role : second  
block-status : unblock  
link-status : UP

topo index 3 :  
host name : Master  
eips type : master  
eips status : FAULT  
border : NO  
base MAC : 0014.0000.1202  
sys oid : 1.3.6.1.4.1.5651.1.102.127  
interface1 : gi0/2  
MAC : 0014.0000.1202  
role : second  
block-status : unblock  
link-status : UP  
interface2 : gi0/1  
MAC : 0014.0000.1202  
role : primary  
block-status : unblock  
link-status : UP

topo index 4 :  
host name : Transit1  
eips type : transit  
eips status : LINK-DOWN  
border : YES  
base MAC : 0001.7a54.5d71

```
sys oid      : 1.3.6.1.4.1.5651.1.102.145
interface1   : gi0/1
  MAC        : 0001.7a54.5d71
  role       : primary
  block-status : unblock
  link-status : UP
interface2   : gi0/2
  MAC        : 0001.7a54.5d71
  role       : second
  block-status : block
  link-status : DOWN
```

Transit1#show eips topology ring 2

ring ID : 2

topo status : round

topo index 1 :

```
  host name   : Transit2
  eips type   : assistant
  eips status  : LINK-UP
  border      : NO
  base MAC    : 0001.7a22.2224
  sys oid     : 1.3.6.1.4.1.5651.1.0.0
  interface2  : gi0/3
  MAC         : 0001.7a22.2224
  role        : edge
  block-status : unblock
  link-status : UP
```

topo index 2 :

```
  host name   : sTransit1
  eips type   : transit
  eips status  : LINK-UP
  border      : NO
  base MAC    : 2012.1209.1728
  sys oid     : 1.3.6.1.4.1.5651.1.102.126
  interface1  : gi0/2
  MAC         : 2012.1209.1728
  role        : second
  block-status : unblock
  link-status : UP
  interface2  : gi0/1
```

```

MAC      : 2012.1209.1728
role     : primary
block-status : unblock
link-status : UP
topo index 3 :
host name : sMaster
eips type : master
eips status : COMPLETE
border   : NO
base MAC : 0000.0010.0017
sys oid  : 1.3.6.1.4.1.5651.1.102.140
interface1 : gi0/2
MAC      : 0000.0010.0017
role     : second
block-status : block
link-status : UP
interface2 : gi0/1
MAC      : 0000.0010.0017
role     : primary
block-status : unblock
link-status : UP
topo index 4 :
host name : Transit1
eips type : edge
eips status : LINK-UP
border   : NO
base MAC : 0001.7a54.5d71
sys oid  : 1.3.6.1.4.1.5651.1.102.145
interface1 : gi0/3
MAC      : 0001.7a54.5d71
role     : edge
block-status : unblock
link-status : UP

```

#When only the link between the subring's transmission node sTransit1 and the assistant edge node Transit2 is disconnected, you can see on the edge node Transit1 and assistant edge node Transit2 through show eips topology that the status of subring Ring2 is not round, EIPS status of subring's master node sMaster becomes FAULT, slave port gigabitethernet0/2 of the subring's master node sMaster is unblocked, and sTransit1 can communicate with Transit2 through the subring's master node sMaster to ensure the communication between sTransit1 and Transit2 is uninterrupted; the status of main ring Ring1 is still round,

the EIPS status is still COMPLETE, and the slave port gigabitethernet0/2 of master node Master is still blocked.

```
Transit1#show eips topology ring 2
ring ID      : 2
topo status  : not round
topo index 1 :
  host name   : sTransit1
  eips type   : transit
  eips status : LINK-DOWN
  border      : NO
  base MAC    : 2012.1209.1728
  sys oid     : 1.3.6.1.4.1.5651.1.102.126
  interface1  : gi0/2
    MAC       : 2012.1209.1728
    role      : second
    block-status : block
    link-status : DOWN
  interface2  : gi0/1
    MAC       : 2012.1209.1728
    role      : primary
    block-status : unblock
    link-status : UP
topo index 2 :
  host name   : sMaster
  eips type   : master
  eips status : FAULT
  border      : NO
  base MAC    : 0000.0010.0017
  sys oid     : 1.3.6.1.4.1.5651.1.102.140
  interface1  : gi0/2
    MAC       : 0000.0010.0017
    role      : second
    block-status : unblock
    link-status : UP
  interface2  : gi0/1
    MAC       : 0000.0010.0017
    role      : primary
    block-status : unblock
    link-status : UP
topo index 3 :
```

host name : Transit1  
eips type : edge  
eips status : LINK-UP  
border : NO  
base MAC : 0001.7a54.5d71  
sys oid : 1.3.6.1.4.1.5651.1.102.145  
interface1 : gi0/3  
MAC : 0001.7a54.5d71  
role : edge  
block-status : unblock  
link-status : UP

Transit2#show eips topology ring 2

ring ID : 2  
topo status : not round  
topo index 1 :  
host name : Transit2  
eips type : assistant  
eips status : LINK-DOWN  
border : NO  
base MAC : 0001.7a22.2224  
sys oid : 1.3.6.1.4.1.5651.1.0.0  
interface1 : gi0/3  
MAC : 0001.7a22.2224  
role : edge  
block-status : block  
link-status : DOWN

Transit1#show eips topology ring 1

ring ID : 1  
topo status : round  
topo index 1 :  
host name : Transit2  
eips type : transit  
eips status : LINK-UP  
border : YES  
base MAC : 0001.7a22.2224  
sys oid : 1.3.6.1.4.1.5651.1.0.0  
interface1 : gi0/1  
MAC : 0001.7a22.2224  
role : primary  
block-status : unblock

```
link-status : UP
interface2 : gi0/2
MAC : 0001.7a22.2224
role : second
block-status : unblock
link-status : UP
topo index 2 :
host name : Transit3
eips type : transit
eips status : LINK-UP
border : NO
base MAC : 0000.0000.008b
sys oid : 1.3.6.1.4.1.5651.1.102.146
interface1 : gi0/1
MAC : 0000.0000.008b
role : primary
block-status : unblock
link-status : UP
interface2 : gi0/2
MAC : 0000.0000.008b
role : second
block-status : unblock
link-status : UP
topo index 3 :
host name : Master
eips type : master
eips status : COMPLETE
border : NO
base MAC : 0014.0000.1202
sys oid : 1.3.6.1.4.1.5651.1.102.127
interface1 : gi0/2
MAC : 0014.0000.1202
role : second
block-status : block
link-status : UP
interface2 : gi0/1
MAC : 0014.0000.1202
role : primary
block-status : unblock
link-status : UP
```

topo index 4 :

host name : Transit1  
eips type : transit  
eips status : LINK-UP  
border : YES  
base MAC : 0001.7a54.5d71  
sys oid : 1.3.6.1.4.1.5651.1.102.145  
interface1 : gi0/1  
MAC : 0001.7a54.5d71  
role : primary  
block-status : unblock  
link-status : UP  
interface2 : gi0/2  
MAC : 0001.7a54.5d71  
role : second  
block-status : unblock  
link-status : UP

# 102 ULPP and Monitor Link

---

## 102.1 Overview

Dual-uplink networking mode is one of the frequently-used networking modes in core networks. This networking mode improves network reliability through redundant link. Generally, STP is used to remove redundant links. However, the convergence time of STP cannot meet the requirement of carrier Ethernet. In this circumstance, ULPP (UpLink Protect Protocol) was born.

ULPP means UpLink Protect Protocol. In addition to satisfying users' requirement for fast convergence of link, it achieves redundant backup of host and backup links and rapid switch of traffic, and effectively simplifies the configuration, making both deployment and maintenance more convenient and improving the working efficiency of deployment and maintenance staff.

Monitor Link provides coordination management technology for changes of link status. There are multiple uplink ports and multiple downlink ports in Monitor Link group. The uplink ports are monitored in real time. When their status changes, the downlink ports are coordinated to quickly notify the status of uplink device port to downlink device. This can help STP, ULPP and other modules rapidly respond to network changes and traffic switch.

## 102.2 ULPP Function Configuration

Table 102 ULPP Function Configuration List

Configuration Task	
Configure Basic Functions of ULPP	Configure ULPP Group
	Configure Uplink Port of ULPP
Configure ULPP Compatible Mode	Configure Compatible Mode of ULPP Group

Configuration Task	
	Configure Compatible Mode of ULPP Uplink Port
Configure Basic Functions of Monitor Link	Configure Monitor Link Group

### 102.2.1 Configure Basic Functions of ULPP

#### Configuration Condition

Before configuring the basic functions of ULPP, first complete the following tasks:

- Configure the spanning tree instance mapping relationship of ULPP group;
- This VLAN has been created when the control VLAN of ULPP group is configured;
- The member ports in ULPP group must be added to the VLAN.

#### Configure ULPP Group

There are two ports in ULPP group, i.e. master port and backup port. The ULPP group has two working modes: link backup and load sharing. In link backup mode, either master or backup port in the ULPP group can be in forwarding status, and the other is blocked, in standby state. When the port in normal forwarding status has any link failure, the ULPP group will automatically block this port, and switch the status of the originally blocked standby port to forwarding. In the load sharing mechanism, the ULPP group carries spanning tree instance traffic in different VLANs according to the binding relationship between the spanning tree instance configured on the master/backup port and the port.

Table 102 Configuring ULPP Group

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Create ULPP group and enter the ULPP configuration mode	<b>ulpp-group</b> <i>group-id</i>	Mandatory By default, ULPP group is not created.
Configure the master port of ULPP group	<b>master { interface</b> <i>interface-name</i>   <b>interface link-aggregation</b> <i>link-aggregation-id</i> }	Mandatory

Step	Command	Description
		By default, master port of the ULPP group is not configured.
Configure backup port of ULPP group	<b>slave</b> { <b>interface</b> <i>interface-name</i>   <b>interface link-aggregation</b> <i>link-aggregation-id</i> }	Mandatory By default, backup port of the ULPP group is not configured.
Configure the stance carried by ULPP group	<b>instance group</b> <i>instance-number</i> { <b>master</b>   <b>slave</b> }	Mandatory By default, the stance carried by ULPP group is not configured.  The spanning tree instances carried by master port and backup port shall not intersect with each other.
Configure the control VLAN of ULPP group	<b>control-vlan</b> <i>vlan-id</i>	Mandatory By default, control VLAN of the ULPP group is not configured.
Configure ULPP group enablement	<b>enable</b>	Mandatory By default, ULPP group enablement is not configured.
Enable the FLUSH packet sending function of ULPP group	<b>flush enable</b>	Optional By default, the FLUSH packet sending function of ULPP group is not enabled.
Configure the working mode of ULPP group	<b>mode</b> { <b>load-balance</b>   <b>backup</b> }	Optional By default, the ULPP group is in master/backup mode.
Configure role preemption	<b>preemption mode role</b>	Optional

Step	Command	Description
function for ULPP group		By default, the role preemption of ULPP group is not configured.  Only when the working mode of ULPP group is link backup will the role preemption function be configured.

## Note

- EIPS, STP and loopback detection functions must be disabled on the member ports of ULPP group.
- The member ports of ULPP group shall not be those of the ULPP group and Monitor Link group that have existed.
- The control VLAN in ULPP group shall not be used to forward service data.
- One ULPP group has one control VLAN only, and one control VLAN belongs to one ULPP group only.
- After the ULPP group is disabled, member ports are all blocked in all spanning tree instances.

### Configure Uplink Port of ULPP

When the ULPP group has link switch, the ULPP group notifies other devices to refresh their address tables by sending FLUSH packet to them so as to ensure the rapid switch of service traffic in the network. In addition to receiving FLUSH packet, the uplink port forwards FLUSH packet within the control VLAN of the device.

Table 102 Configuring Control VLAN for Uplink Port of ULPP Group

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the port configuration mode	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2 Ethernet interface configuration mode, the

Step	Command	Description
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation link-aggregation-id</b>	subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Configure control VLAN for uplink port of ULPP group	<b>ulpp flush control-vlan vlan-list</b>	Mandatory  By default, the control VLAN for uplink port of ULPP group is not configured.

## 102.2.2 Configure ULPP Compatible Mode

### Configuration Condition

Before configuring ULPP compatible mode, ensure that:

- To configure ULPP compatible mode, basic functions of ULPP group need to be configured;
- To configure the compatible mode of ULPP uplink mode, the control VLAN of ULPP uplink port needs to be configured first.

### Configure Compatible Mode of ULPP Group

ULPP group has three compatible modes, i.e. flexlink, smartlink, and smartlink multicast-mode.

Table 1 Configuring Compatible Mode of ULPP Group

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the ULPP configuration mode	<b>ulpp-group group-id</b>	-
Configure Compatible Mode of ULPP Group	<b>compatible { flexlink   smartlink   smartlink multicast-mode }</b>	Mandatory  By default, the compatible mode of ULPP group is not configured.

## Configure Compatible Mode of ULPP Uplink Port

ULPP uplink port has three compatible modes, i.e. flexlink, smartlink, and smartlink multicast-mode.

Table 2 Configuring Compatible Mode of ULPP Uplink Port

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Configure compatible mode of ULPP uplink port	<b>ulpp compatible</b> { <b>flexlink</b>   <b>smartlink</b>   <b>smartlink multicast-mode</b> }	Mandatory  By default, the compatible mode for uplink port of ULPP group is not configured.

---

### Note

- Compatible mode can be configured only when the spanning tree of uplink port in ULPP group is closed.
- 

## 102.2.3 Configure Basic Functions of Monitor Link Group

### Configuration Condition

None

### Configure Monitor Link Group

The Monitor Link group may have multiple uplink ports, such as general port, member port of aggregation group, aggregation group, VSL port or ULPP group. The Monitor Link group may have multiple downlink ports, such as general port, member port of aggregation group, and aggregation group. But ULPP group cannot serve as a downlink port.

Table 3 Configuring Creation of Monitor Link

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Create Monitor Link group and enter the Monitor Link configuration mode	<b>mtlk-group</b> <i>group-id</i>	Mandatory By default, Monitor Link group is not created.
Configure the uplink port of Monitor Link group	<b>uplink</b> { <b>interface</b> <i>interface-name</i>   <b>interface link-aggregation</b> <i>link-aggregation-id</i>   <b>ulpp-group</b> <i>group-id</i> }	Optional By default, uplink port of Monitor Link group is not configured.
Configure the downlink port of Monitor Link group	<b>downlink</b> { <b>interface</b> <i>interface-name</i>   <b>interface link-aggregation</b> <i>link-aggregation-id</i> }	Optional By default, downlink port of Monitor Link group is not configured.

### 102.2.4 ULPP Monitoring and Maintaining

Table 102 ULPP Monitoring and Maintaining

Command	Description
<b>clear ulpp message flush</b> { <b>receive</b>   <b>send</b> <i>group group-id</i>   <b>transmit</b> }	Clear the statistics of FLUSH packets of ULPP group
<b>show ulpp group</b> <i>group-id</i>	Show the configurations of ULPP group
<b>show ulpp instance group</b> <i>group-id</i>	Show the status of the spanning tree carried by master/backup member port in ULPP group

Command	Description
<b>show ulpp message flush</b> { send group <i>group-id</i>   receive   transmit }	Show the statistics of FLUSH packets processed by ULPP group
<b>show ulpp assi</b>	Show the configurations of uplink port of ULPP group
<b>show mtlk group</b> <i>group-id</i>	Show the configurations of Monitor Link group

## 102.3 Typical Configuration Example of ULPP and Monitor Link

### 102.3.1 Configure ULPP

#### Network Requirements

- Four devices constitute a dual-uplink network. In particular, uplink devices include Device1, Device2, and Device3, and Device4 is a downlink device.
- ULPP function is configured for the downlink device so that the port can normally carry or switch the services in associated spanning tree instance.

#### Network Topology

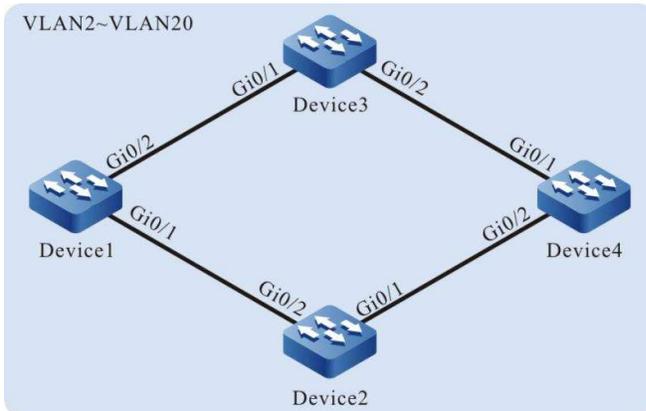


Figure 102 Configuring Network Topology of ULPP

#### Configuration Steps

Step 1: Configure VLANs and the link type of the ports.

#On Device1, create VLAN2-VLAN20, and configure the link type of ports gigabitEthernet0/1 and gigabitEthernet0/2 as Trunk to allow services of VLAN2-VLAN20 to pass.

```
Device1#configure terminal
Device1(config)#vlan 2-20
Device1(config)#interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#switchport mode trunk
Device1(config-if-gigabitethernet0/1)#switchport trunk allowed vlan add 2-20
Device1(config-if-gigabitethernet0/1)#exit
Device1(config)#interface gigabitethernet 0/2
Device1(config-if-gigabitethernet0/2)#switchport mode trunk
Device1(config-if-gigabitethernet0/2)#switchport trunk allowed vlan add 2-20
Device1(config-if-gigabitethernet0/2)#exit
```

---

## Note

- The VLAN and configuration of port link type on Device2, Device3, and Device 4 are the same as those on Device1. (Omitted)
- 

Step 2: #Configure spanning tree instance on Device4.

#Configure spanning tree instance. Map instance 1 to VLAN3~VLAN10 and instance 2 to VLAN11~VLAN20.

```
Device4(config)#spanning-tree mst configuration
Device4(config-mst)#region-name admin
Device4(config-mst)#revision-level 1
Device4(config-mst)#instance 1 vlan 3-10
Device4(config-mst)#instance 2 vlan 11-20
```

#Enable the spanning tree instance.

```
Device4(config-mst)#active configuration pending
Device4(config-mst)#exit
```

Step 3: #Configure ULPP function on Device4.

#Create ULPP group.

```
Device4(config)#ulpp-group 1
```

#Configure the master port gigabitethernet0/1 and slave port gigabitethernet0/2 of ULPP group.

```
Device4(config-ulpp-1)#master interface gigabitethernet 0/1
Device4(config-ulpp-1)#slave interface gigabitethernet 0/2
```

#Configure associated spanning tree instance 1 of master port gigabitethernet0/1 and associated spanning tree instance 2 of slave port gigabitethernet0/2.

```
Device4(config-ulpp-1)#instance group 1 master
Device4(config-ulpp-1)#instance group 2 slave
```

#Configure the working mode of ULPP group as link backup.

```
Device4(config-ulpp-1)#mode backup
```

#Configure the control VLAN of ULPP group as VLAN2.

```
Device4(config-ulpp-1)#control-vlan 2
```

#Enable the Flush packet sending mechanism of ULPP.

```
Device4(config-ulpp-1)#flush enable
```

#Enable ULPP group.

```
Device4(config-ulpp-1)#enable  
Device4(config-ulpp-1)#exit
```

---

## Note

- After VLAN2 is configured as a control VLAN, it only permits Flush packet to pass.
- 

Step 4: Configure uplink devices Device1, Device2, and Device3.

#Configure Flush packet receiving and forwarding mechanism on Device1.

```
Device1(config)#interface gigabitethernet 0/1-0/2  
Device1(config-if-range)#ulpp flush control-vlan 2  
Device1(config-if-range)#exit
```

---

## Note

- The packet receiving and sending mechanism of Device2 and Device3, is the same as that of Device1. (Omitted)
- 

Step 5: Check the results.

#View the status of ULPP group on Device4.

```
Device4#show ulpp group 1  
-----  
ulpp-group 1 configuration information  
-----  
Current status      : MASS  
Work type           : Backup  
Control vlan        : 2  
Flush function       : Enable  
Preemption mode     : Disable  
Master interface name : gi0/1  
Slave interface name  : gi0/2  
Master interface status : Active  
Slave interface status : Standby  
Master interface instance : 1  
Slave interface instance : 2  
Flexlink compatible  : Disable  
Smartlink compatible  : Disable
```

```
Smartlink mcast compatible : Disable
Enable status              : Enable
```

#On Device4, view the status of associated spanning tree instances of master and slave ports.

```
Device4#show ulpp instance group 1
-----
ulpp-group 1 instance status
-----
Master forwarding instance : 1-2
Master block instance     : None
Slave forwarding instance  : None
Slave block instance      : 1-2
```

#When the port gigabitethernet0/1 of Device4 fails, the status of ULPP group will be switched. View the status of ULPP group on Device4.

```
Device4#show ulpp group 1
-----
ulpp-group 1 configuration information
-----
Current status      : MNSA
Work type          : Backup
Control vlan       : 2
Flush function     : Enable
Preemption mode    : Disable
Master interface name : gi0/1
Slave interface name : gi0/2
Master interface status : Down
Slave interface status : Active
Master interface instance : 1
Slave interface instance : 2
Flexlink compatible : Disable
Smartlink compatible : Disable
Smartlink mcast compatible : Disable
Enable status      : Enable
```

The master port gigabitethernet0/1 changes from Active to Down, and the slave port gigabitethernet0/2 changes from Standby to Active. The services in spanning tree instance are normally forwarded through gigabitethernet0/2.

#The uplink devices Device1 and Device2 will print the following information.

```
19:26:10: [tUlp] %ULPP-ASSI: Receive flush message from gigabitethernet0/2 success, the receive sequence number is 1, vlan id is 2
```

This is the information of Flush packet received by uplink devices Device1 and Device2 when the status of ULPP group changes.

## 102.3.2 Configure Monitor Link

### Network Requirements

- Four devices constitute a dual-uplink network. In particular, uplink devices include Device1, Device2, and Device3, and Device4 is a downlink device.
- Configure the Monitor Link function on Device3 to achieve link status monitoring.
- When the uplink port of Monitor Link group fails, the downlink port is closed, which

causes the ULPP group to switch between active and standby links to ensure network connectivity.

### Network Topology

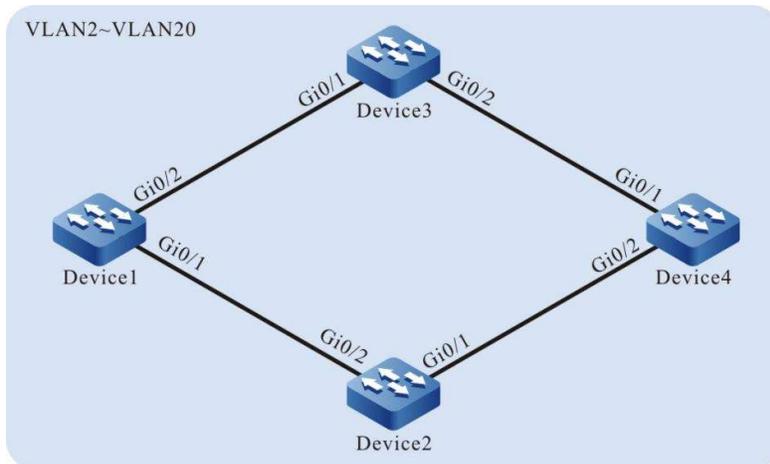


Figure 102 Configuring Network Topology of Monitor Link

### Configuration Steps

Step 1: Configure VLANs and the link type of the ports.

#On Device1, create VLAN2-VLAN20, and configure the link type of ports gigabitethernet0/1 and gigabitethernet0/2 as Trunk to allow services of VLAN2-VLAN20 to pass.

```
Device1#configure terminal
Device1(config)#vlan 2-20
Device1(config)#interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#switchport mode trunk
Device1(config-if-gigabitethernet0/1)#switchport trunk allowed vlan add 2-20
Device1(config-if-gigabitethernet0/1)#exit
Device1(config)#interface gigabitethernet 0/2
Device1(config-if-gigabitethernet0/2)#switchport mode trunk
Device1(config-if-gigabitethernet0/2)#switchport trunk allowed vlan add 2-20
Device1(config-if-gigabitethernet0/2)#exit
```

---

### Note

- The configuration of port and link type on Device2, Device3, and Device 4 is the same as that on Device1. (Omitted)
- 

Step 2: #Configure spanning tree instance on Device4.

#Configure spanning tree instance. Map instance 1 to VLAN3~VLAN10 and instance 2 to VLAN11~VLAN20.

```
Device4(config)#spanning-tree mst configuration
```

```
Device4(config-mst)#region-name admin
Device4(config-mst)#revision-level 1
Device4(config-mst)#instance 1 vlan 3-10
Device4(config-mst)#instance 2 vlan 11-20
```

#Enable the spanning tree instance.

```
Device4(config-mst)#active configuration pending
Device4(config-mst)#exit
```

Step 3: #Configure ULPP function on Device4.

```
Device4(config)#ulpp-group 1
Device4(config-ulpp-1)#master interface gigabitethernet 0/1
Device4(config-ulpp-1)#slave interface gigabitethernet 0/2
Device4(config-ulpp-1)#instance group 1 master
Device4(config-ulpp-1)#instance group 2 slave
Device4(config-ulpp-1)#mode backup
Device4(config-ulpp-1)#control-vlan 2
Device4(config-ulpp-1)#flush enable
Device4(config-ulpp-1)#enable
Device4(config-ulpp-1)#exit
```

---

## Note

- After VLAN2 is configured as a control VLAN, it only permits Flush packet to pass.
- 

Step 4: Configure uplink devices Device1, Device2, and Device3.

#Configure Flush packet receiving and forwarding mechanism on Device1.

```
Device1(config)#interface gigabitethernet 0/1-0/2
Device1(config-if-range)#ulpp flush control-vlan 2
Device1(config-if-range)#exit
```

---

## Note

- The packet receiving and sending mechanism of Device2 and Device3, is the same as that of Device1. (Omitted)
- 

Step 5: Configure Monitor Link group.

#Configure Monitor Link group on Device3.

```
Device3(config)#mtlk-group 1
```

#On Device3, configure gigabitethernet0/1 as the uplink port of Monitor Link.

```
Device3(config-mtlk-1)#uplink interface gigabitethernet 0/1
```

#On Device3, configure gigabitethernet0/2 as the downlink port of Monitor Link.

```
Device3(config-mtlk-1)#downlink interface gigabitethernet 0/2
```

#View Monitor Link group.

```
Device3#show mtlk group 1
-----
mtlk-group 1 configuration information
-----
Uplink interface      : gi0/1
Uplink type           : no-ulpp
Uplink status         : up
Downlink interface    : gi0/2
```

Step 6: Check the result.

#When the uplink port gigabitethernet0/1 of the uplink device Device3 fails, the status of downlink port gigabitethernet0/2 coordinates with that of uplink port gigabitethernet 0/1, and the downlink port is forced to be closed.

#View the status of the downlink port gigabitethernet0/2.

```
Device3#show interface gigabitethernet 0/2
gigabitethernet0/2 configuration information
  Description      : downlink
  Status           : Enabled
  Link             : Down (Err-disabled)
  Set Speed        : Auto
  Act Speed        : Unknown
  Set Duplex       : Auto
  Act Duplex       : Unknown
  Set Flow Control : Off
  Act Flow Control : Off
  Mdx              : Auto
  Mtu              : 1824
  Port mode        : LAN
  Port ability     : 10M HD,10M FD,100M HD,100M FD,1000M FD
  Link Delay       : No Delay
  Storm Control    : Unicast Disabled
  Storm Control    : Broadcast Disabled
  Storm Control    : Multicast Disabled
  Storm Action     : None
  Port Type        : Nni
  Pvid             : 1
  Set Medium       : Copper
  Act Medium       : Copper
  Mac Address      : 0001.7a58.000b
```

After the downlink port gigabitethernet0/2 is closed, the ULPP group of Device4 switches between active and standby links to ensure network connectivity

# 103 VRRP

---

## 103.1 Overview

VRRP is the short name for Virtual Router Redundancy Protocol. In short, VRRP is a fault tolerance protocol. It can ensure when the next-hop device of the host fails, it can be timely replaced by another device to ensure the continuity and reliability of communication. To enable the VRRP to work, first you need to create a virtual IP address and MAC address to add a virtual device to this network. The host on this network can communicate with the virtual device without knowing any information of the physical device on this network.

- A virtual device is composed of a master device and several backup devices. The master device can implements forwarding function. When the master device fails, the backup device becomes a new master device to continue to perform its task. The master and backup devices are hereinafter referred to as "Master" and "Backup" respectively.

## 103.2 VRRP Function Configuration

Table 103-1 VRRP Function Configuration List

Configuration Task	
Configure Basic Functions of VRRP	Enable VRRP Protocol
	Configure VRRP Priority
	Configure VRRP Preemption Mode
	Configure Real MAC Address of VRRP
Configure VRRP Coordination Group	Configure VRRP Coordination Group

Configuration Task	
Configure VRRP Network Authentication	Configure Simple Text Authentication for VRRP
Configure VRRP Delay Downgrading	Configure VRRP Delay Downgrading
Configure VRRP Packet Dispersion	Configure VRRP Packet Dispersion
Configure VRRP Delayed Recovery	Configure VRRP Delayed Recovery
Configure Virtual MAC Address of VRRP dual-holding	Configure Virtual MAC Address of VRRP dual-holding
Configure Static VRRP Function	Configure Static VRRP
Configure Association of VRRP with Track	Configure Coordination of VRRP with Track to Monitor Uplink of Master
	Configure Coordination of VRRP with Track to Monitor Interconnecting Lines of Master and Backup

### 103.2.1 Configure Basic Functions of VRRP

Among various configuration tasks of VRRP, VRRP must be enabled first. Other functional performance configured cannot take effect until the virtual IP address of VRRP group is in the same network segment with the interface IP address.

#### Configuration Condition

Before configuring the basic VRRP functions, do the following:

- Configure interface IP address.

#### Enable VRRP Protocol

To enable VRRP functions, you are required to create a VRRP group under the interface and configure virtual IP address.

Table 103-2 Enabling VRRP

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	Mandatory
Configure VRRP group	<b>vrrp vrid ip</b> <i>ip-address</i>	Mandatory Enable VRRP. In particular, vrid is the VRRP group number, and ip-address is the virtual IP address.

### Configure VRRP Priority

After VRRP is configured, if no priority is set, the default priority 100 will be used; the device with a higher priority will be elected as the Master responsible for forwarding packets, and others will become Backups; if all devices have the same priority, the election will be conducted according to the size of the interface IP address of each device, and the device with a larger interface IP address becomes the Master. You can set the priority of VRRP as needed. The larger the value, the higher the priority.

Table 103-3 Configuring VRRP Priority

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	Mandatory
Configure the priority of VRRP group	<b>vrrp vrid priority</b> <i>priority</i>	Mandatory Configure VRRP priority. The default priority is 100.

### Note

- In virtual MAC mode, when the interface IP address is the same as the virtual IP address, it becomes Init immediately, and the priority remains unchanged. If the user wants the virtual IP address to be the same as the interface IP address, it needs to change the virtual

---

MAC mode to real MAC mode.

---

### Configure VRRP Preemption Mode

Configure VRRP. In preemption mode, once other devices in VRRP group finds their priority is higher than that of current Master, they will become the Master; in non-preemption mode, if the Master doesn't fail, other devices cannot become a Master even if they are configured with higher priority.

Table 103-4 Configuring VRRP Preemption Mode

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	Mandatory
Configure VRRP group as preemption mode	<b>vrrp vrid preempt</b>	Mandatory By default, the preemption mode is enabled.

### Configure Real MAC Address of VRRP

The virtual device in a VRRP group has one virtual MAC address. According to RFC2338, the format of the virtual MAC address is as follows: 00-00-5E-00-01-{vrid}. When the virtual device responds to an ARP request, it provides a virtual MAC address instead of a real MAC address of the interface. It is noteworthy that virtual MAC address of interface is used by default.

Table 2 Configuring Real MAC Address of VRRP

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	Mandatory
Configure real MAC address for VRRP	<b>vrrp vrid use-bia</b>	Mandatory By default, virtual MAC address is used.

---

 **Note**

- By default, virtual MAC address is used after VRRP configuration. When the commands mentioned in this section are configured, real MAC address is used by the host to forward packets; after deleting these commands, the virtual MAC address is used by the host to forward packets.
- 

### 103.2.2 Configure VRRP Coordination Group

VRRP coordination group can reduce the interaction between VRRP protocol packets, alleviate network load, and reach millisecond switch. When multiple common VRRP groups are added to a VRRP coordination group, they play different roles in this coordination group, such as Active or non-Active. The Active group instead of non-Active group sends protocol packets. The non-Active group has the same status as the Active group, i.e. the former switches with the latter, in order to reduce interaction of protocol packets. Millisecond sending period of VRRP packets can be configured for the coordination group to meet the purpose of rapid switch.

#### Configuration Condition

Before configuring the VRRP coordination group, do the following:

- Configure multiple VRRP groups.

#### Configure VRRP Coordination Group

To configure a VRRP coordination group, first create one, and then add the common VRRP group configured to the coordination group created. The common VRRP group can be added to the coordination group as an Active group or a non-Active group. But one coordination group must have only one Active group.

Table 103-6 Configuring VRRP Coordination Group

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure coordination group	<b>vrrp linkgroup</b> <i>lgid</i> [ <b>interval</b> <i>Interval-time</i> ]	Mandatory The default value of interval-time is 1000ms.
Enter interface mode.	<b>interface</b> <i>interface-name</i>	Mandatory

Step	Command	Description
Add the common VRRP group to the coordination group as an Active group	<b>vrrp vrid linkgroup lgid</b> [ <b>active</b> ]	Mandatory  If [active] is not selected, it will be added as a non-Active group.

## Note

- In addition to coordination group, multiple VRRP groups can be used to achieve load balancing. For details, see the chapter "Configure VRRP Load Balancing" in "VRRP Typical Configuration Example".
- In coordination group, when common VRRP group is added, the common group timer will fail. That is to day, the sending period of VRRP packet in common group is subject to the timer of the coordination group.

### 103.2.3 Configure VRRP Network Authentication

VRRP supports simple text authentication which requires no more than 8 digits of authentication key.

#### Configuration Condition

Before configuring VRRP network authentication, ensure that:

- Configure a VRRP group.

#### Configure Simple Text Authentication for VRRP

Table 103-7 Configuring VRRP Simple Text Authentication

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	Mandatory
Configure Simple Text Authentication for VRRP	<b>vrrp vrid authentication text</b> <i>string</i>	Mandatory

Step	Command	Description
		By default, the simple text authentication function is disabled.  The authentication key should have no more than 8 characters.

### 103.2.4 Configure VRRP Delay Downgrading

In order to meet the requirements of high reliability scenario, delay downgrading function can be configured for VRRP. When the device status of VRRP switches from Master to Backup, it can forward service traffic within the time of delay downgrading so as to effectively avoid losing service traffic due to the slow traffic switch of downstream switch equipment. The Backup device still under delay degradation can forward the service traffic with destination MAC address being a virtual MAC address. Therefore, the Backup device will also forward traffic packets when the delay downgrading timer takes effect, causing double traffic to be sent. This function is not recommended if there is a low requirement for reliability to prevent double traffic from affecting the network.

#### Configuration Condition

Before configuring the VRRP delay downgrading function, ensure that:

- Configure a VRRP group.

#### Configure VRRP Delay Downgrading

Table 103-8 Configuring VRRP Delay Downgrading

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	Mandatory
Configure VRRP Delay Downgrading	<b>vrrp vrid degrade-delay</b> <i>delay-time</i>	Mandatory  Configure VRRP delay downgrading. In particular, vrid is the VRRP group number, and delay-time is

Step	Command	Description
		the delay downgrading time.

### 103.2.5 Configure VRRP Packet Dispersion

In order to meet the requirements of high reliability scenario, the VRRP packet dispersion function can be configured when a large number of VRRP groups are configured. When VRRP bursts, the VRRP packet sending time is discretized to ensure balanced sending of VRRP packets.

#### Configuration Condition

No.

#### Configure VRRP Packet Dispersion

Table 103-9 Configuring VRRP Packet Dispersion

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure VRRP Packet Dispersion	<b>vrrp disperse- skew skew-time</b>	Mandatory Configure VRRP packet dispersion. Skew-time is the packet dispersion interval.

### 103.2.6 Configure VRRP Delayed Recovery

In order to meet the requirements of high reliability scenario, the VRRP delayed recovery function can be configured. When the interface status of VRRP device switches from down to up, VRRP switches status after delayed recovery in INIT status.

#### Configuration Condition

Before configuring VRRP delayed recovery function, do the following:

- Configure a VRRP group.

Configure VRRP Packet Dispersion

Table 103-10 Configuring VRRP Delayed Recovery

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure VRRP Delayed Recovery	<b>vrp restore-delay</b> <i>delay-time</i>	Mandatory Configure VRRP delayed recovery. Delay-time is the VRRP recovery delay time.

### 103.2.7 Configure Virtual MAC Address of VRRP dual-holding

In order to meet the requirements of high reliability scenario, virtual MAC dual-holding function can be configured for VRRP. When the Master fails, and the device status of VRRP has not switched from Backup to Master yet, the Backup device can rapidly start the forwarding of service traffic to effectively reduce the time of gateway blackhole. However, under normal conditions, if the downstream switch device has flooding of service traffic, the Backup device with mac dual-holding enabled will also forward traffic packets, causing double traffic to be sent. This function is not recommended if there is a low requirement for reliability to prevent double traffic from affecting the network.

#### Configuration Condition

Before configuring VRRP virtual MAC dual-holding function, do the following:

- Configure a VRRP group.
- This VRRP group uses virtual MAC address.

Configure VRRP Packet Dispersion

Table 103-11 Configuring VRRP Virtual MAC Dual-holding

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	Mandatory
Configure Virtual MAC Address of VRRP dual-holding	<b>vrp vrid</b> <i>svlm</i>	Mandatory Configure VRRP virtual MAC dual-holding. In particular,

Step	Command	Description
		vrid is the VRRP group number.

### 103.2.8 Configure Static VRRP Function

After the static VRRP function is enabled, VRRP doesn't perform protocol interaction, the status will ultimately remain at master, and ARP responses can be given normally. This applies to single-device virtual gateways and MLAG scenarios.

#### Configuration Condition

Before configuring static VRRP function, do the following:

- Configure a VRRP group.

#### Configure Static VRRP Function

Table 103-12 Configuring Static VRRP

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	Mandatory
Configure Static VRRP	<b>vrrp</b> <i>vrid</i> <b>static</b>	Mandatory Configure static VRRP. In particular, vrid is the VRRP group number.

### 103.2.9 Configure Coordination of VRRP with Track

VRRP can monitor the status of uplink and the line connecting Master and Backup to improve the reliability of VRRP.

#### Configuration Condition

Before configuring the coordination of VRRP with Track, do the following:

- Configure a VRRP group.

### Configure Coordination of VRRP with Track to Monitor Uplink of Master

Configure coordination with Track on the Master. By associating the interface or BFD and RTR through Track, you can make it focus on the status of uplink interface. If the uplink interface is down, VRRP can reduce the priority of the Master with the consumption value configured. At this time, upon receipt, the Backup will automatically switch to Master (it is worth noting that the priority of Master is lower than that of Backup at this time). If it's necessary to switch to Backup quickly, you can configure the command of fast switch upon receipt of low-priority packet on the Backup. For details, see the figure below.

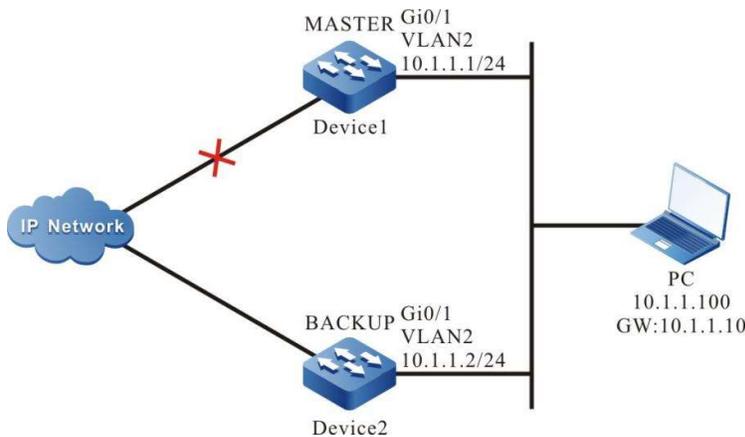


Figure 103-1 Configuring Coordination of VRRP with Track to Monitor Uplink of Master

### Configure Coordination of VRRP with Track to Associate Uplink Interface

Associate VRRP with the uplink interface to be cared about through Track. When the uplink interface is down, the Master will automatically lower its priority and the Backup will receive the VRRP packet with a low priority and switch to Master; if the user has configured "fast switch upon receipt of low-priority packet", i.e. "low-pri-master" function, the Backup will quickly switch to Master.

Table 3 Configuring Coordination of VRRP with Track to Associate with Uplink Interface (Configured on Master)

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter interface mode.	<b>interface</b> <i>interface-name</i>	Mandatory
Configure association of VRRP with uplink interface	<b>vrrp vrid track</b> <i>interface-name</i> [ <i>decrement</i> ]	Mandatory By default, the priority consumption value is 10.
Configure the function of fast switch after VRRP	<b>vrrp vrid switchover low-pri-master</b>	Optional

Step	Command	Description
receives low-priority packet		This command is configured on the Backup for fast switch after the priority of Master decreases.

### Configure Coordination of VRRP with Track (Associate Track with BFD and RTR)

If Track is associated with BFD and RTR, the Master can directly associate with this Track to monitor the lines. When any failure occurs on the lines, the Master decreases its priority. At this moment, the Backup switches to Master after receiving the VRRP packet with a low priority. If the user configures the "fast switch upon receipt of low-priority packet", i.e. "low-pri-master" function, the Backup will quickly switch to Master.

Table 103-14 Configuring Coordination of Master with Track (Associate Track with BFD and RTR)

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter interface mode.	<b>interface</b> <i>interface-name</i>	Mandatory
Configure association of VRRP with uplink interface	<b>vrrp vrid track track-id</b> [ <i>decrement</i> ]	Mandatory By default, the priority consumption value is 10.
Configure the function of fast switch after VRRP receives low-priority packet	<b>vrrp vrid switchover low-pri-master</b>	Optional This command is configured on the Backup for fast switch after the priority of Master decreases.

### Note

- For the creation of Track and the configurations of Association of Track with BFD or RTR, see Track-related chapter in the User Manual.
- The low-pri-master function enables the Backup to switch quickly when receiving low-priority packets, even if it is in non-preemption mode. If this function is not configured,

when low-priority packets are received, the Backup will switch after the next timeout period. When the switch time is not strictly required, it's unnecessary to configure the low-pri-master function. However, when the switch time is strictly required, this function can make the switch time reach millisecond level.

### Configure Coordination of VRRP with Track to Monitor Interconnecting Lines of Master and Backup

After coordination of VRRP with Track to monitor interconnecting lines of Master and Backup is configured, when the line between Master and Backup is down, the Backup will quickly switch to Master. For details, see the figure below.

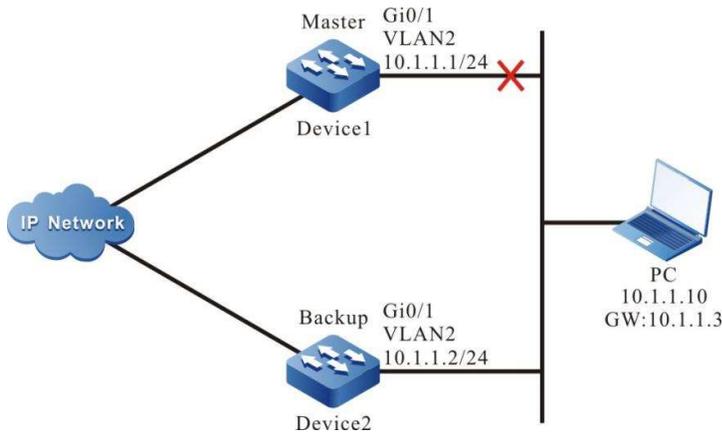


Figure 103-2 Configuring Coordination of VRRP with Track to Monitor Interconnecting Lines of Master and Backup

Table 103-15 Configuring Coordination of VRRP with Track to Monitor Interconnecting Lines of Master and Backup

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter interface mode.	<b>interface <i>interface-name</i></b>	Mandatory
Configure the function of fast switch when the Backup VRRP device finds the line between Master and Backup becomes down	<b>vrrp vrid track track-id switchover</b>	Mandatory

---

## Note

- For the configurations of associating Track with BFD and RTR, see Track-related chapter in the User Manual.
  - Track can be associated with BFD to monitor the interconnecting lines between Master and Backup.
- 

### 103.2.10 VRRP Monitoring and Maintaining

Table 103-16 VRRP Monitoring and Maintaining

Command	Description
<b>show vrrp</b> [ <b>brief</b> ]   [ <b>interface</b> <i>interface-name</i> ]   [ <b>group</b> [ <i>linkgroup-number</i> ]]	Show the VRRP configuration information, including virtual IP address, virtual MAC address, device status, device priority, dependent device interface address, and coordination group.

## 103.3 Typical Configuration Example of VRRP

### 103.3.1 Configure the Priority of Single VRRP Backup Group

#### Network Requirements

- On Device1 and Device2, create a single VRRP backup group so that Device1 and Device2 can share a virtual IP address to back up the default gateway of the user's host, reducing the time of network disconnection.

#### Network Topology

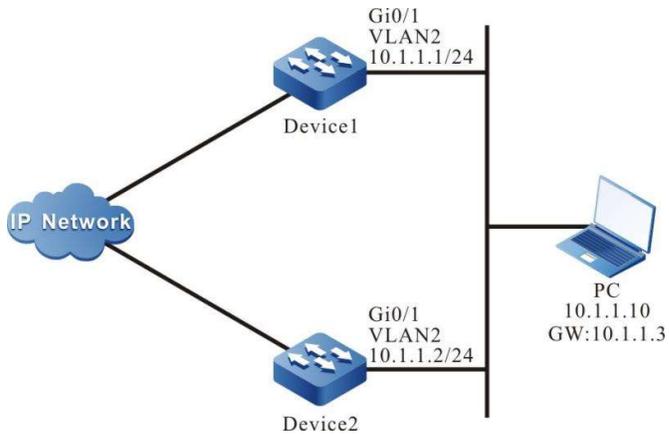


Figure 103-3 Network Topology for Configuring Single VRRP Backup Group

### Configuration Steps

Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configure IP addresses for the ports. (Omitted)

Step 3: Configure a VRRP group.

#On Device1, configure VRRP group 1, with virtual IP address of 10.1.1.3 and priority configured of 110.

```
Device1#configure terminal
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#vrrp 1 ip 10.1.1.3
Device1(config-if-vlan2)#vrrp 1 priority 110
Device1(config-if-vlan2)#exit
```

#On Device2, configure VRRP group 1, with virtual IP address of 10.1.1.3.

```
Device2#configure terminal
Device2(config)#interface vlan 2
Device2(config-if-vlan2)#vrrp 1 ip 10.1.1.3
Device2(config-if-vlan2)#exit
```

Step 4: Check the result.

#View the VRRP status of Device1.

```
Device1#show vrrp
Interface vlan2 (Flags 0x1)
Pri-addr : 10.1.1.1
Vrf : 0
Virtual router : 1
Virtual IP address : 10.1.1.3
Virtual MAC address : 00-00-5e-00-01-01 , installed into HW
Depend prefix:10.1.1.1/24
State : Master
Normal priority : 110
Currnet priority : 110
Priority reduced : 0
Preempt-mode : YES
Advertise-interval : 1 s
```

Authentication Mode : None

#View the VRRP status of Device2.

```
Device2#show vrrp
Interface vlan2 (Flags 0x1)
Pri-addr : 10.1.1.2
Vrf : 0
Virtual router : 1
Virtual IP address : 10.1.1.3
Virtual MAC address : 00-00-5e-00-01-01
Depend prefix:10.1.1.2/24
State : Backup
Master addr : 10.1.1.1
Normal priority : 100
Current priority : 100
Priority reduced : 0
Preempt-mode : YES
Advertise-interval : 1 s
Authentication Mode : None
```

It can be seen that the VRRP status of Device1 is Master, and that of Device2 is Backup. Device1 shares a virtual IP address with Device2. The host communicates with the network through this address. When Device1 fails, Device2 immediately switches to Master for data forwarding.

---

## Note

- For VRRP status, the device with a higher priority is the Master. When they have the same priority, the device with a larger interface IP address is the Master.
  - By default, VRRP works in preemption mode, and the default priority is 100.
- 

### 103.3.2 Configure VRRP Coordination Group

#### Network Requirements

- Enable VRRP on Device1 and Device2 interfaces, and add it to the coordination group. Only the Active group in the coordination group exchanges protocol packets.
- The VRRP status in non-Active group maintains the same as that of Active group, i.e. the status of Active group switches with the change of non-Active group.

#### Network Topology

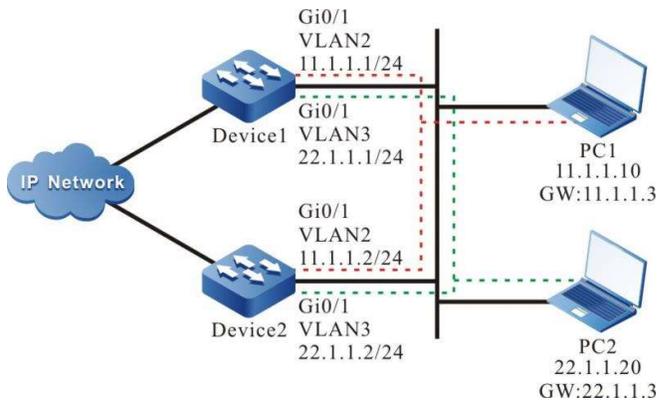


Figure 103 Network Topology for Configuring Multiple VRRP Backup Groups

### Configuration Steps

Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configure IP addresses for the ports. (Omitted)

Step 3: Configure a VRRP coordination group.

#Configure a VRRP coordination group on Device1.

```
Device1#configure terminal
Device1(config)#vrrp linkgroup 1
```

#On Device2, configure VRRP coordination group 1.

```
Device2#configure terminal
Device2(config)#vrrp linkgroup 1
```

Step 4: Configure a VRRP Group.

#On the interface of Device1, configure the virtual IP address of VRRP group 1 as 11.1.1.3.

```
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#vrrp 1 ip 11.1.1.3
Device1(config-if-vlan2)#exit
```

#On the interface of Device1, configure the virtual IP address of VRRP group 2 as 22.1.1.3.

```
Device1(config)#interface vlan 3
Device1(config-if-vlan3)#vrrp 2 ip 22.1.1.3
Device1(config-if-vlan3)#exit
```

#On the interface of Device2, configure the virtual IP address of VRRP group 1 as 11.1.1.3.

```
Device2(config)#interface vlan 2
Device2(config-if-vlan2)#vrrp 1 ip 11.1.1.3
Device2(config-if-vlan2)#exit
```

#On the interface of Device2, configure the virtual IP address of VRRP group 2 as 22.1.1.3.

```
Device2(config)#interface vlan 3
Device2(config-if-vlan3)#vrrp 2 ip 22.1.1.3
```

```
Device2(config-if-vlan3)#exit
```

Step 5: Add VRRP to the coordination group.

#On Device1, add VRRP group 1 to the coordination group as an Active group.

```
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#vrrp 1 linkgroup 1 active
Device1(config-if-vlan2)#exit
```

#On Device1, add VRRP group 2 to the coordination group as a non-Active group.

```
Device1(config)#interface vlan 3
Device1(config-if-vlan3)#vrrp 2 linkgroup 1
Device1(config-if-vlan3)#exit
```

#On Device2, add VRRP group 1 to the coordination group as an Active group.

```
Device2(config)#interface vlan 2
Device2(config-if-vlan2)#vrrp 1 linkgroup 1 active
Device2(config-if-vlan2)#exit
```

#On Device2, add VRRP group 2 to the coordination group as a non-Active group.

```
Device2(config)#interface vlan 3
Device2(config-if-vlan3)#vrrp 2 linkgroup 1
Device2(config-if-vlan3)#exit
```

Step 6: Check the result.

#View the VRRP status on Device1.

```
Device1#show vrrp
Interface vlan2 (Flags 0x1)
Pri-addr : 11.1.1.1
Vrf : 0
Virtual router : 1
Linkgroup : 1
Active : TRUE
Virtual IP address : 11.1.1.3
Virtual MAC address : 00-00-5e-00-01-01
Depend prefix:11.1.1.1/24
State : Backup
Master addr : 11.1.1.2
Normal priority : 100
Curmet priority : 100
Priority reduced : 0
Preempt-mode : YES
Advertise-interval : 1 s
Authentication Mode : None

Interface vlan3 (Flags 0x1)
Pri-addr : 22.1.1.1
Vrf : 0
Virtual router : 2
Linkgroup : 1
Active : FALSE
Virtual IP address : 22.1.1.3
Virtual MAC address : 00-00-5e-00-01-02
Depend prefix:22.1.1.1/24
State : Backup
Master addr : 0.0.0.0
```

```
Normal priority : 100
Currnet priority : 100
Priority reduced : 0
Preempt-mode : YES
Advertise-interval : 1 s
Authentication Mode : None
```

#View the VRRP status on Device2.

```
Device2#show vrrp
Interface vlan2 (Flags 0x1)
Pri-addr : 11.1.1.2
Vrf : 0
Virtual router : 1
Linkgroup : 1
Active : TRUE
Virtual IP address : 11.1.1.3
Virtual MAC address : 00-00-5e-00-01-01 , installed into HW
Depend prefix:11.1.1.2/24
State : Master
Normal priority : 100
Currnet priority : 100
Priority reduced : 0
Preempt-mode : YES
Advertise-interval : 1 s
Authentication Mode : None

Interface vlan3 (Flags 0x1)
Pri-addr : 22.1.1.2
Vrf : 0
Virtual router : 2
Linkgroup : 1
Active : FALSE
Virtual IP address : 22.1.1.3
Virtual MAC address : 00-00-5e-00-01-02 , installed into HW
Depend prefix:22.1.1.2/24
State : Master
Normal priority : 100
Currnet priority : 100
Priority reduced : 0
Preempt-mode : YES
Advertise-interval : 1 s
Authentication Mode : None
```

It is indicated that the VRRP status of non-Active group is consistent with that of Active group.

Step 7: Configure the priority of VLAN2 on Device1 as 110 for status switch.

```
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#vrrp 1 priority 110
Device1(config-if-vlan2)#exit
```

#View the VRRP status on Device1.

```
Device1#show vrrp
Interface vlan2 (Flags 0x1)
Pri-addr : 11.1.1.1
Vrf : 0
Virtual router : 1
Linkgroup : 1
Active : TRUE
Virtual IP address : 11.1.1.3
Virtual MAC address : 00-00-5e-00-01-01 , installed into HW
Depend prefix:11.1.1.1/24
State : Master
Normal priority : 110
Currnet priority : 110
Priority reduced : 0
Preempt-mode : YES
Advertise-interval : 1 s
```

Authentication Mode : None

```
Interface vlan3 (Flags 0x1)
Pri-addr : 22.1.1.1
Vrf : 0
Virtual router : 2
Linkgroup : 1
Active : FALSE
Virtual IP address : 22.1.1.3
Virtual MAC address : 00-00-5e-00-01-02 , installed into HW
Depend prefix:22.1.1.1/24
State : Master
Normal priority : 100
Curmet priority : 100
Priority reduced : 0
Preempt-mode : YES
Advertise-interval : 1 s
Authentication Mode : None
```

#View the VRRP status on Device2.

```
Device2#show vrrp
Interface vlan2 (Flags 0x1)
Pri-addr : 11.1.1.2
Vrf : 0
Virtual router : 1
Linkgroup : 1
Active : TRUE
Virtual IP address : 11.1.1.3
Virtual MAC address : 00-00-5e-00-01-01
Depend prefix:11.1.1.2/24
State : Backup
Master addr : 11.1.1.1
Normal priority : 100
Curmet priority : 100
Priority reduced : 0
Preempt-mode : YES
Advertise-interval : 1 s
Authentication Mode : None
```

```
Interface vlan3 (Flags 0x1)
Pri-addr : 22.1.1.2
Vrf : 0
Virtual router : 2
Linkgroup : 1
Active : FALSE
Virtual IP address : 22.1.1.3
Virtual MAC address : 00-00-5e-00-01-02
Depend prefix:22.1.1.2/24
State : Backup
Master addr : 0.0.0.0
Normal priority : 100
Curmet priority : 100
Priority reduced : 0
Preempt-mode : YES
Advertise-interval : 1 s
Authentication Mode : None
```

It can be seen that the status of non-Active group changes with that of Active group. The Active group instead of non-Active group in the coordination group is responsible for sending protocol packets. This can significantly reduce the interactions between VRRP protocol packets and the network load.



- 
- The sending interval of the coordination group can be as short as millisecond level to meet the purpose of rapid switch.
- 

### 103.3.3 Configure Coordination of VRRP with Track

#### Network Requirements

- VRRP is enabled between Device1 and Device2 so that Device1 and Device2 can share a virtual IP address to back up the default gateway of the user's host.
- Device1 monitors the status of VLAN3 through Track. When the uplink interface VLAN3 of Device1 is down, VRRP can sense and switch status so that the Backup will become a Master for data forwarding.

#### Network Topology

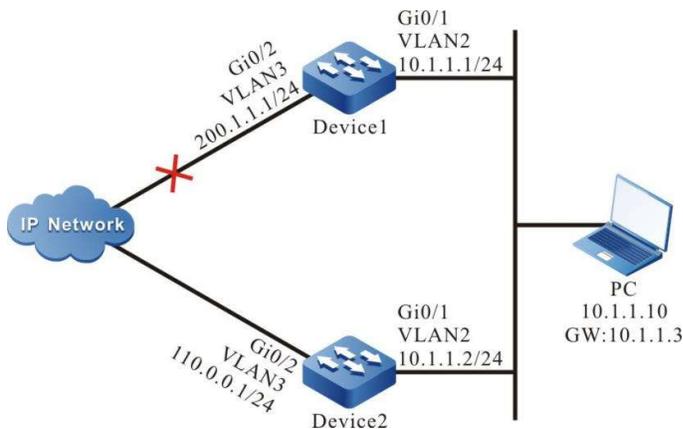


Figure 1 Network Topology for Configuring Coordination of VRRP with Track

#### Configuration Steps

- Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)
- Step 2: Configure IP addresses for the ports. (Omitted)
- Step 3: Configure a VRRP group.

#On Device1, configure VRRP group 1, with virtual IP address of 10.1.1.3 and priority of 110.

```
Device1#configure terminal
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#vrrp 1 ip 10.1.1.3
Device1(config-if-vlan2)#vrrp 1 priority 110
Device1(config-if-vlan2)#exit
```

#On Device2, configure VRRP group 1, with virtual IP address of 10.1.1.3.

```
Device2#configure terminal
Device2(config)#interface vlan 2
Device2(config-if-vlan2)#vrrp 1 ip 10.1.1.3
Device2(config-if-vlan2)#exit
```

#View the VRRP status of Device1.

```
Device1#show vrrp
Interface vlan2 (Flags 0x1)
Pri-addr : 10.1.1.1
Vrf : 0
Virtual router : 1
Virtual IP address : 10.1.1.3
Virtual MAC address : 00-00-5e-00-01-01 , installed into HW
Depend prefix:10.1.1.1/24
State : Master
Normal priority : 110
Curmet priority : 110
Priority reduced : 0
Preempt-mode : YES
Advertise-interval : 1
Authentication Mode : None
```

#View the VRRP status of Device2.

```
Device2#show vrrp
Interface vlan2 (Flags 0x1)
Pri-addr : 10.1.1.2
Vrf : 0
Virtual router : 1
Virtual IP address : 10.1.1.3
Virtual MAC address : 00-00-5e-00-01-01
Depend prefix:10.1.1.2/24
State : Backup
Master addr : 10.1.1.1
Normal priority : 100
Curmet priority : 100
Priority reduced : 0
Preempt-mode : YES
Advertise-interval : 1
Authentication Mode : None
```

Step 4: Configure coordination of VRRP with Track.

#On Device1, configure coordination of VRRP with Track to monitor the uplink interface VLAN3, and configure the priority decrement as 20.

```
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#vrrp 1 track vlan3 20
Device1(config-if-vlan2)#exit
```

#View the VRRP status of Device1.

```
Device1#show vrrp
Interface vlan2 (Flags 0x1)
Pri-addr : 10.1.1.1
Vrf : 0
Virtual router : 1
Virtual IP address : 10.1.1.3
Virtual MAC address : 00-00-5e-00-01-01 , installed into HW
Depend prefix:10.1.1.1/24
State : Master
Normal priority : 110
Curmet priority : 110
Priority reduced : 0
Preempt-mode : YES
```

```
Advertise-interval : 1
Authentication Mode : None
Track interface : vlan3
Reduce : 20
Reduce state : NO
```

When the uplink interface VLAN3 of Device1 is down, VRRP priority decreases by 20. As a result, Device2 has a higher priority, which causes status switch.

#View the VRRP status of Device1.

```
Device1#show vrrp
Interface vlan2 (Flags 0x1)
Pri-addr : 10.1.1.1
Vrf : 0
Virtual router : 1
Virtual IP address : 10.1.1.3
Virtual MAC address : 00-00-5e-00-01-01
Depend prefix:10.1.1.1/24
State : Backup
Master addr : 10.1.1.2
Normal priority : 110
Curmet priority : 90
Priority reduced : 20
Preempt-mode : YES
Advertise-interval : 1
Authentication Mode : None
Track interface : vlan3
Reduce : 20
Reduce state : YES
```

#View the VRRP status of Device2.

```
Device2#show vrrp
Interface vlan2 (Flags 0x1)
Pri-addr : 10.1.1.2
Vrf : 0
Virtual router : 1
Virtual IP address : 10.1.1.3
Virtual MAC address : 00-00-5e-00-01-01 , installed into HW
Depend prefix:10.1.1.2/24
State : Master
Normal priority : 100
Curmet priority : 100
Priority reduced : 0
Preempt-mode : YES
Advertise-interval : 1
Authentication Mode : None
```

---

## Note

- For the purpose of fast switch during coordination of VRRP with Track, you can configure switchover low-pri-master on the Backup.
- 

### 103.3.4 Configure Coordination of VRRP with BFD

#### Network Requirements

- Enable VRRP between Device1 and Device2.
- It at least takes 3s for the VRRP status to switch between Device1 and Device2, which means a very long period of service disconnection. Coordination of VRRP with BFD is required to be configured on Device1 and Device2 to achieve millisecond switch.

### Network Topology

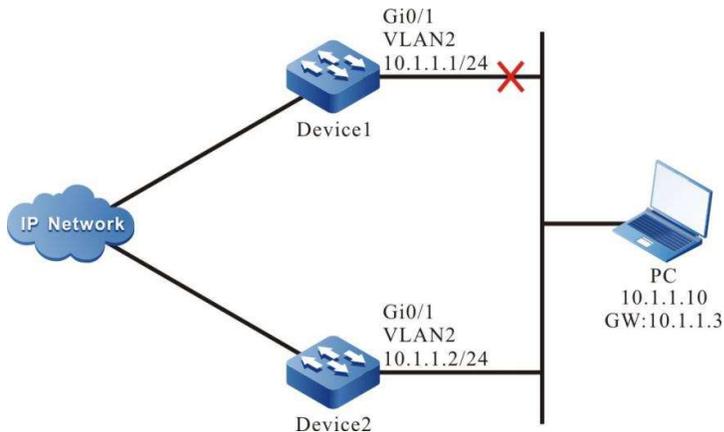


Figure 2 Network Topology for Configuring Coordination of VRRP with BFD

### Configuration Steps

Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configure IP addresses for the ports. (Omitted)

Step 3: Configure a VRRP group.

#On Device1, configure VRRP group 1, with virtual IP address of 10.1.1.3 and priority configured of 105.

```
Device1#configure terminal
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#vrrp 1 ip 10.1.1.3
Device1(config-if-vlan2)#vrrp 1 priority 105
Device1(config-if-vlan2)#exit
```

#On Device2, configure VRRP group 1, with virtual IP address of 10.1.1.3.

```
Device2#configure terminal
Device2(config)#interface vlan 2
Device2(config-if-vlan2)#vrrp 1 ip 10.1.1.3
Device2(config-if-vlan2)#exit
```

#View the VRRP status of Device1.

```
Device1#show vrrp
Interface vlan2 (Flags 0x1)
Pri-addr : 10.1.1.2
Vrf : 0
Virtual router : 1
Virtual IP address : 10.1.1.3
Virtual MAC address : 00-00-5e-00-01-01 , installed into HW
Depend prefix:10.1.1.2/24
State : Master
Normal priority : 105
```

```
Curmet priority : 105
Priority reduced : 0
Preempt-mode : YES
Advertise-interval : 1 s
Authentication Mode : None
```

#View the VRRP status of Device2.

```
Device2#show vrrp
Interface vlan2 (Flags 0x1)
Pri-addr : 10.1.1.2
Vrf : 0
Virtual router : 1
Virtual IP address : 10.1.1.3
Virtual MAC address : 00-00-5e-00-01-01
Depend prefix:10.1.1.2/24
State : Backup
Master addr : 10.1.1.1
Normal priority : 100
Curmet priority : 100
Priority reduced : 0
Preempt-mode : YES
Advertise-interval : 1 s
Authentication Mode : None
```

Step 4: Configure the coordination of Track with BFD.

#Configure coordination of Track with BFD on Device1.

```
Device1(config)#track 1
Device1(config-track)#bfd interface vlan2 remote-ip 10.1.1.2 local-ip 10.1.1.1
Device1(config-track)#exit
```

#Configure coordination of Track with BFD on Device2.

```
Device2#configure terminal
Device2(config)#track 1
Device2(config-track)#bfd interface vlan2 remote-ip 10.1.1.1 local-ip 10.1.1.2
Device2(config-track)#exit
```

#View BFD status on Device1.

```
Device1#show bfd session
OurAddr      NeighAddr      LD/RD      State      Holddown      interface
10.1.1.1      10.1.1.2      6/7        UP         5000          vlan2
```

#View BFD status on Device2.

```
Device2#show bfd session
OurAddr      NeighAddr      LD/RD      State      Holddown      interface
10.1.1.2      10.1.1.1      7/6        UP         5000          vlan2
```

Step 5: Configure coordination of VRRP with Track.

#On Device2, configure coordination of VRRP with Track, and configure switchover.

```
Device2(config)#interface vlan 2
Device2(config-if-vlan2)#vrrp 1 track 1 switchover
Device2(config-track)#exit
```

Step 6: Check the result.

#View the VRRP status on Device2.

```
Device2#show vrrp
Interface vlan2 (Flags 0x1)
Pri-addr : 10.1.1.1
Vrf : 0
Virtual router : 1
Virtual IP address : 10.1.1.3
Virtual MAC address : 00-00-5e-00-01-01
Depend prefix:10.1.1.1/24
State : Backup
Master addr : 10.1.1.2
Normal priority : 100
Curmet priority : 100
Priority reduced : 0
Preempt-mode : YES
Advertise-interval : 1 s
Authentication Mode : None
Track object : 1
Switchover state : NO
```

When the line of Device1 fails, the BFD session is down, so is Track. Device2 can immediately sense and switch to Master for data forwarding.

#View the status of BFD and VRRP on Device2.

```
Device2#show bfd session
OurAddr      NeighAddr      LD/RD      State      Holddown      interface
10.1.1.2      10.1.1.1      7/0        DOWN        5000          vlan2
Device2#show vrrp
Interface vlan2 (Flags 0x1)
Pri-addr : 10.1.1.2
Vrf : 0
Virtual router : 1
Virtual IP address : 10.1.1.3
Virtual MAC address : 00-00-5e-00-01-01 , installed into HW
Depend prefix:10.1.1.2/24
State : Master
Normal priority : 100
Curmet priority : 100
Priority reduced : 0
Preempt-mode : YES
Advertise-interval : 1 s
Authentication Mode : None
Track object : 1
Switchover state : YES
```

---

## Note

- When VRRP coordinates with Track, Switchover needs to be configured on the Backup. Once Track down is detected, it will switch to Master immediately.
-

### 103.3.5 Configure VRRP load balancing

#### Network Requirements

- Device1 and Device2 belong to two different VRRP groups. In particular, Device1 is a Master in group 1 and a Backup in group 2; Device2 is a Backup in group 1 and a Master in group 2.
- PC1 forwards data through Device1, and PC2 does so through Device2 to realize load balancing.

#### Network Topology

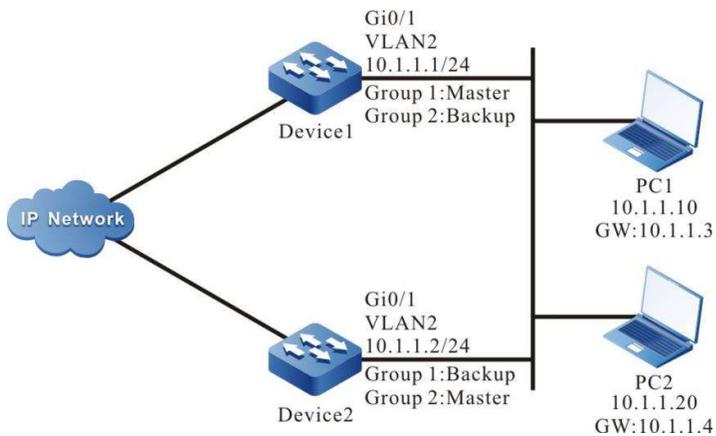


Figure 3 Network Topology for VRRP Load Balancing

#### Configuration Steps

Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configure IP addresses for the ports. (Omitted)

Step 3: Create VRRP group 1.

#On Device1, configure VRRP group 1, with virtual IP address of 10.1.1.3 and priority configured of 110.

```
Device1#configure terminal
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#vrrp 1 ip 10.1.1.3
Device1(config-if-vlan2)#vrrp 1 priority 110
Device1(config-if-vlan2)#exit
```

#On Device2, configure VRRP group 1, with virtual IP address of 10.1.1.3.

```
Device2#configure terminal
Device2(config)#interface vlan 2
Device2(config-if-vlan2)#vrrp 1 ip 10.1.1.3
Device2(config-if-vlan2)#exit
```

Step 4: Create VRRP group 2.

#On Device1, configure the virtual IP address of VRRP group 2 as 10.1.1.4.

```
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#vrrp 2 ip 10.1.1.4
Device1(config-if-vlan2)#exit
```

#On Device2, configure the virtual IP address of VRRP group 2 as 10.1.1.4 and the priority as 110.

```
Device2(config)#interface vlan 2
Device2(config-if-vlan2)#vrrp 2 ip 10.1.1.4
Device2(config-if-vlan2)#vrrp 2 priority 110
Device2(config-if-vlan2)#exit
```

Step 5: Check the result.

#On Device1, view VRRP status in group 1 and 2.

```
Device1#show vrrp
Interface vlan2 (Flags 0x1)
Pri-addr : 10.1.1.1
Vrf : 0
Virtual router : 1
Virtual IP address : 10.1.1.3
Virtual MAC address : 00-00-5e-00-01-01 , installed into HW
Depend prefix:10.1.1.1/24
State : Master
Normal priority : 110
Currnet priority : 110
Priority reduced : 0
Preempt-mode : YES
Advertise-interval : 1 s
Authentication Mode : None

Virtual router : 2
Virtual IP address : 10.1.1.4
Virtual MAC address : 00-00-5e-00-01-02
Depend prefix:10.1.1.1/24
State : Backup
Master addr : 10.1.1.2
Normal priority : 100
Currnet priority : 100
Priority reduced : 0
Preempt-mode : YES
Advertise-interval : 1 s
Authentication Mode : None
```

#On Device2, view VRRP status in group 1 and 2.

```
Device2#show vrrp
Interface vlan2 (Flags 0x1)
Pri-addr : 10.1.1.2
Vrf : 0
Virtual router : 1
Virtual IP address : 10.1.1.3
Virtual MAC address : 00-00-5e-00-01-01
Depend prefix:10.1.1.2/24
State : Backup
Master addr : 10.1.1.1
Normal priority : 100
Currnet priority : 100
Priority reduced : 0
Preempt-mode : YES
```

Advertise-interval : 1 s  
Authentication Mode : None

Virtual router : 2  
Virtual IP address : 10.1.1.4  
Virtual MAC address : 00-00-5e-00-01-02 , installed into HW  
Depend prefix:10.1.1.2/24  
State : Master  
Normal priority : 110  
Current priority : 110  
Priority reduced : 0  
Preempt-mode : YES  
Advertise-interval : 1 s  
Authentication Mode : None

It is indicated that as a Master of VRRP group 1, Device1 also acts as a Backup in VRRP group 2. On the contrary, as a Master of VRRP group 2, Device2 also acts as a Backup in VRRP group 1. When a device fails, the two PCs forward data through the other one. This can achieve both load balancing and mutual backup.

# 104 VRRPv3

## 104.1 Overview

VRRPv3 is the short name for Virtual Router Redundancy Protocol Version 3. In short, VRRPv3 is a fault tolerance protocol. It can ensure when the next-hop device of the host fails, it can be timely replaced by another device to ensure the continuity and reliability of communication. To enable the VRRPv3 to work, first you need to create a virtual IP address and MAC address to add a virtual device to this network. The host on this network can communicate with the virtual device without knowing any information of the physical device on this network. A virtual device is composed of a master device and several backup devices. The master device can implements forwarding function. When the master device fails, the backup device becomes a new master device to continue to perform its task.

The master and backup devices are hereinafter referred to as "Master" and "Backup" respectively.

## 104.2 VRRPv3 Function Configuration

Table 104 VRRPv3 Function Configuration List

Configuration Task	
Configure Basic Functions of VRRPv3	Enable VRRPv3 Protocol
	Configure VRRPv3 Priority
	Configure VRRPv3 Preemption Mode
	Configure Virtual MAC Address of VRRPv3
Configure Static VRRPv3 Functions	Configure Static VRRPv3
Configure Association of VRRPv3 with Track	Configure Coordination of VRRPv3 with Track to Monitor Uplink of Master
	Configure Coordination of VRRPv3 with Track to Monitor Interconnecting Lines of Master and Backup

## 104.2.1 Configure Basic Functions of VRRPv3

In various configuration tasks of VRRPv3, you must enable VRRPv3 first. For the virtual IPv6 link-local address of VRRPv3 group, other functional performance configured cannot take effect until the IPv6 link-local address of interface is enabled.

### Configuration Condition

Before configuring the basic VRRPv3 functions, do the following:

- Enable the IPv6 link-local address of interface.

### Enable VRRPv3 Protocol

To enable VRRPv3 functions, you are required to create a VRRPv3 group under the interface and configure IPv6 link-local virtual address. If global virtual address needs to be configured, the network segment of this virtual address must be the same as that of the global real address on the interface.

Table 1 Enabling VRRPv3 Protocol

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	Mandatory
Configure link-local virtual address of VRRPv3 group	<b>ipv6 vrrp vrid ip ip-address link-local</b>	Mandatory By default, VRRPv3 is not enabled.
Configure global virtual address of VRRPv3 group	<b>ipv6 vrrp vrid ip ip-address</b>	Optional The global virtual address configured must be in the same network segment with the global real address on the interface. By default, global virtual address is disabled.

### Configure VRRPv3 Priority

After VRRPv3 is configured, if no priority is set, the default priority 100 will be used; the device with a higher priority will be elected as the Master responsible for forwarding packets, and others will become

Backups; if all devices have the same priority, the election will be conducted according to the size of the interface IPv6 link-local address of each device, and the device with a larger interface IPv6 link-local address becomes the Master. You can set the priority of VRRPv3 as needed. The larger the value, the higher the priority.

Table 2 Configuring VRRPv3 Priority

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	Mandatory
Configure the priority of VRRPv3 group	<b>ipv6 vrrp vrid priority</b> <i>priority</i>	Mandatory By default, the VRRPv3 priority is 100.

### Configure VRRPv3 Preemption Mode

Configure VRRPv3. In preemption mode, once other devices in VRRPv3 group finds their priority is higher than that of current Master, they will become the Master; in non-preemption mode, if the Master doesn't fail, other devices cannot become a Master even if they are configured with higher priority.

Table 104 Configuring VRRPv3 Preemption Mode

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	Mandatory
Configure VRRPv3 group as preemption mode	<b>ipv6 vrrp vrid preempt</b>	Mandatory By default, the preemption function is enabled.

### Configure Real MAC Address of VRRPv3

The virtual router in a VRRPv3 group has one virtual MAC address. According to RFC5798, the format of the virtual MAC address is as follows: 00-00-5E-00-02-{vrid}. It is noteworthy that virtual MAC address is used by default.

Table 3 Configuring Real MAC Address of VRRPv3

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	Mandatory
Configure virtual MAC address fir VRRPv3	<b>ipv6 vrrp vrid use-bia</b>	Mandatory By default, VRRPv3 will use virtual MAC address.

---

### Note

- By default, virtual MAC address is used after VRRPv3 configuration. When the commands mentioned in this section are configured, real MAC address is used by the host to forward packets; after deleting these commands, the virtual MAC address is used by the host to forward packets.
- 

## 104.2.2 Configure Static VRRPv3 Functions

After the static VRRP function is enabled, VRRPv3 doesn't perform protocol interaction, the status will ultimately remain at master, and NA responses can be given normally. This applies to single-device virtual gateways and MLAG scenarios.

### Configuration Condition

Before configuring static VRRPv3 function, do the following:

- Configure a VRRPv3 group.

### Configure Static VRRP Function

Table 104-6 Configuring Static VRRPv3

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface <i>interface-name</i></b>	Mandatory
Configure Static VRRPv3	<b>ipv6 vrrp <i>vrid</i> static</b>	Mandatory Configure static VRRPv3. <i>vrid</i> is the group number of VRRPv3.

### 104.2.3 Configure Coordination of VRRPv3 with Track

VRRPv3 can monitor the status of uplink and the line connecting Master and Backup to improve the reliability of VRRPv3.

#### Configuration Condition

Before configuring the coordination of VRRPv3 with Track, do the following:

- Configure a VRRPv3 group.

#### Configure Coordination of VRRPv3 with Track to Monitor Uplink of Master

Configure coordination with Track on the Master. By associating the interface or BFD and RTR through Track, you can make it focus on the status of uplink interface. If the uplink interface is down, VRRPv3 can reduce the priority of the Master with the consumption value configured. At this time, upon receipt, the Backup will automatically switch to Master (it is worth noting that the priority of Master is lower than that of Backup at this time). If it's necessary to switch to Backup quickly, you can configure the command of fast switch upon receipt of low-priority packet on the Backup. For details, see the figure below.

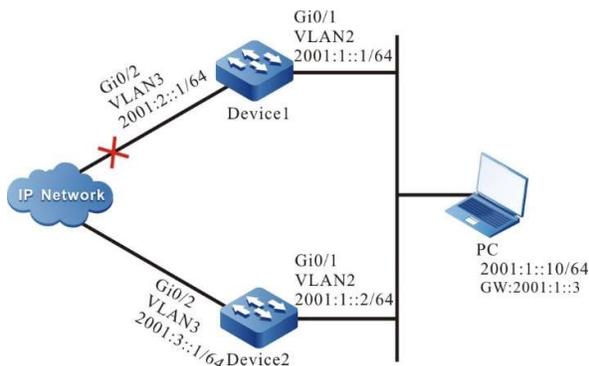


Figure 104-1 Configuring Coordination of VRRPv3 with Track to Monitor Uplink of Master

## Configure Coordination of VRRPv3 with Track to Associate Uplink Interface

Associate VRRPv3 with the uplink interface to be cared about through Track. When the uplink interface is down, the Master will automatically lower its priority and the Backup will receive the VRRPv3 packet with a low priority and switch to Master; if the user has configured "fast switch upon receipt of low-priority packet", i.e. "low-pri-master" function, the Backup will quickly switch to Master.

Table 4 Configuring VRRPv3 to Coordinate Track to Associate with Uplink Interface  
(Configured on Master)

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter interface mode.	<b>interface</b> <i>interface-name</i>	Mandatory
Configure association of VRRPv3 with uplink interface	<b>ipv6 vrrp vrid track</b> <i>interface-name</i> [ <i>decrement</i> ]	Mandatory By default, VRRPv3 is not coordinated with Track.
Configure the function of fast switch after VRRPv3 receives low-priority packet	<b>ipv6 vrrp vrid switchover low-pri-master</b>	Optional By default, the low-pri-master function is disabled.  This command is configured on the Backup for fast switch after the priority of Master decreases.

## Configure VRRPv3 to Coordinate Track (Associate Track with BFD and RTR)

If Track is associated with BFD and RTR, the Master can directly associate with this Track to monitor the lines. When any failure occurs on the lines, the Master decreases its priority. At this moment, the Backup switches to Master after receiving the VRRPv3 packet with a low priority. If the user configures the "fast switch upon receipt of low-priority packet", i.e. "low-pri-master" function, the Backup will quickly switch to Master.

Table 5 Configuring Coordination of Master with Track (Associate Track with BFD and RTR)

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter interface mode.	<b>interface</b> <i>interface-name</i>	Mandatory
Configure association of VRRPv3 with uplink interface	<b>ipv6 vrrp vrid track track-id</b> [ <i>decrement</i> ]	Mandatory By default, VRRPv3 is not coordinated with Track.
Configure the function of fast switch after VRRPv3 receives low-priority packet	<b>ipv6 vrrp vrid switchover low-pri-master</b>	Optional By default, the low-pri-master function is disabled.  This command is configured on the Backup for fast switch after the priority of Master decreases.

---

## Note

- For the creation of Track and the configurations of Association of Track with BFD or RTR, see Track-related chapter in the User Manual.
  - The low-pri-master function enables the Backup to switch quickly when receiving low-priority packets, even if it is in non-preemption mode. If this function is not configured, when low-priority packets are received, the Backup will switch after the next timeout period. When the switch time is not strictly required, it's unnecessary to configure the low-pri-master function. However, when the switch time is strictly required, this function can make the switch time reach millisecond level.
- 

### Configure Coordination of VRRPv3 with Track to Monitor Interconnecting Lines of Master and Backup

After coordination of VRRPv3 with Track to monitor interconnecting lines of Master and Backup is configured, when the line between Master and Backup is down, the Backup will quickly switch to Master. For details, see the figure below.

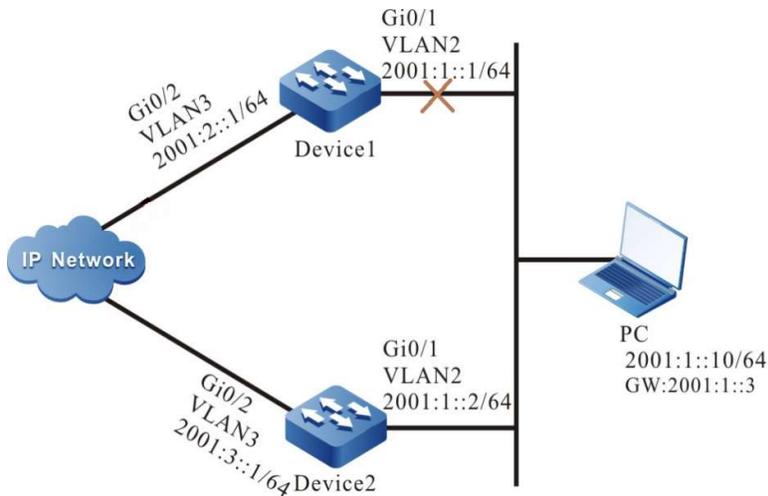


Figure 104-2 Configure Coordination of VRRPv3 with Track to Monitor Interconnecting Lines of Master and Backup

Table 104-9 Configuring Coordination of VRRPv3 with Track to Monitor Interconnecting Lines of Master and Backup

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter interface mode.	<b>interface <i>interface-name</i></b>	Mandatory
Configure the function of fast switch when the Backup VRRPv3 device finds the line between Master and Backup becomes down	<b>ipv6 vrrp <i>vrid</i> track <i>track-id</i> switchover</b>	Mandatory By default, VRRPv3 is not coordinated with Track.

### Note

- For the configurations of associating Track with BFD and RTR, see Track-related chapter in the User Manual.
- Track can be associated with BFD to monitor the interconnecting lines between Master and Backup.

## 104.2.4 VRRPv3 Monitoring and Maintaining

Table 6 VRRPv3 Monitoring and Maintaining

Command	Description
<b>show ipv6 vrrp [ interface <i>interface-name</i> ]   [brief]</b>	Show the VRRPv3 configuration information, including virtual IP address, virtual MAC address, device status, device priority, and dependent device interface address.

## 104.3 Typical Configuration Example of VRRPv3

### 104.3.1 Configure IPv6-based Single VRRP Backup Group

#### Network Requirements

- On Device1 and Device2, create an IPv6-based single VRRP backup group so that Device1 and Device2 can share a virtual IPv6 link-local address and global address to back up the default gateway of the user's host, reducing the time of network disconnection.

#### Network Topology

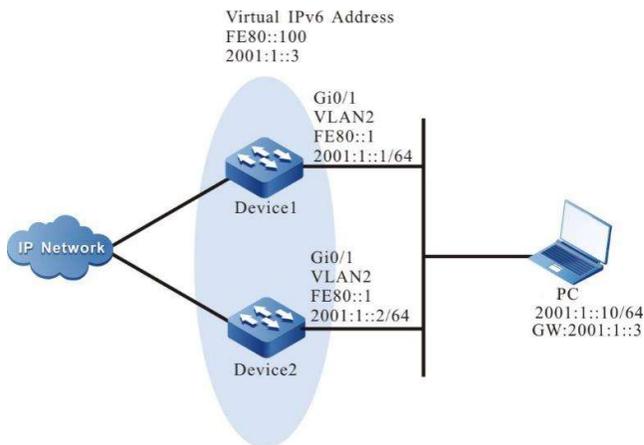


Figure 104-3 Network Topology for Configuring IPv6-based Single VRRP Backup Group

#### Configuration Steps

- Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)
- Step 2: Configure the IPv6 address of each interface, and turn on the switch of RA response and RA period sending.

```
Device1#configure terminal
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ipv6 address fe80::1 link-local
Device1(config-if-vlan2)#ipv6 address 2001:1::1/64
```

```

Device1(config-if-vlan2)#no ipv6 nd suppress-ra period
Device1(config-if-vlan2)#no ipv6 nd suppress-ra response
Device1(config-if-vlan2)#exit
Device2#configure terminal
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ipv6 address fe80::2 link-local
Device2(config-if-vlan2)#ipv6 address 2001:1::2/64
Device2(config-if-vlan2)#no ipv6 nd suppress-ra period
Device2(config-if-vlan2)#no ipv6 nd suppress-ra response
Device2(config-if-vlan2)#exit

```

Step 3: Create an IPv6-based VRRP group.

#On Device1, configure VRRP group 1, with virtual IP address of 2001:1::3 and fe80::100 and priority configured of 110.

```

Device1(config)#interface vlan2
Device1(config-if-vlan2)#ipv6 vrrp 1 ip fe80::100 link-local
Device1(config-if-vlan2)#ipv6 vrrp 1 ip 2001:1::3
Device1(config-if-vlan2)#ipv6 vrrp 1 priority 110
Device1(config-if-vlan2)#exit

```

#On Device2, configure VRRP group 1, with virtual IP address of 2001:1::3 and fe80::100.

```

Device2(config)#interface vlan2
Device2(config-if-vlan2)#ipv6 vrrp 1 ip fe80::100 link-local
Device2(config-if-vlan2)#ipv6 vrrp 1 ip 2001:1::3
Device2(config-if-vlan2)#exit

```

Step 4: Check the result.

#View IPv6 VRRP status on Device1.

```

Device1#show ipv6 vrrp
Interface vlan2 (Flags 0x9)
  Pri-addr : fe80::1
  Vrf : 0
  Pri-matchaddr : fe80::1
  Virtual router : 1
  Mac mode: real mac mode
  Virtual IP address : fe80::100
  Global address count:1
    Global Match address : 2001:1::1
    Global Virtual IP address : 2001:1::3
  Virtual MAC address : 00-00-5e-00-02-01
  State : Master
  Normal priority : 110
  Current priority : 110
  Priority reduced : 0
  Preempt-mode : YES
  Advertise-interval : 100
  Authentication Mode : None

```

#View IPv6 VRRP status on Device2.

```

Device2#show ipv6 vrrp
Interface vlan2 (Flags 0x9)
  Pri-addr : fe80::2
  Vrf : 0
  Pri-matchaddr : fe80::2
  Virtual router : 1
  Mac mode: real mac mode
  Virtual IP address : fe80::100
  Global address count:1
    Global Match address : 2001:1::2
    Global Virtual IP address : 2001:1::3
  Virtual MAC address : 00-00-5e-00-02-01
  State : Backup

```

Master addr : fe80::1  
Normal priority : 100  
Current priority : 100  
Priority reduced : 0  
Preempt-mode : YES  
Advertise-interval : 100  
Authentication Mode : None

It can be seen that the VRRP status of Device1 is Master, and that of Device2 is Backup. Device1 shares a virtual IP address with Device2. The host communicates with the network through this address. When Device1 fails, Device2 immediately switches to Master for data forwarding.

---

## Note

- By default, VRRPv3 works in preemption mode, and the default priority is 100.
  - For VRRPv3 status, the device with a higher priority is the Master. When they have the same priority, the device with a larger interface IP link-local address is the Master.
- 

### 104.3.2 Configure IPv6-based Coordination of VRRP with Track

#### Network Requirements

- On Device1 and Device2, create an IPv6-based single VRRP backup group so that Device1 and Device2 can share a virtual IPv6 link-local address and virtual global address to back up the default gateway of the user's host, reducing the time of network disconnection.
- Device1 monitors the status of VLAN3 through Track. When the uplink interface VLAN3 of Device1 is down, VRRPv3 can sense the down event on the monitoring event and lower its priority so that the Backup will become a Master for data forwarding.

#### Network Topology

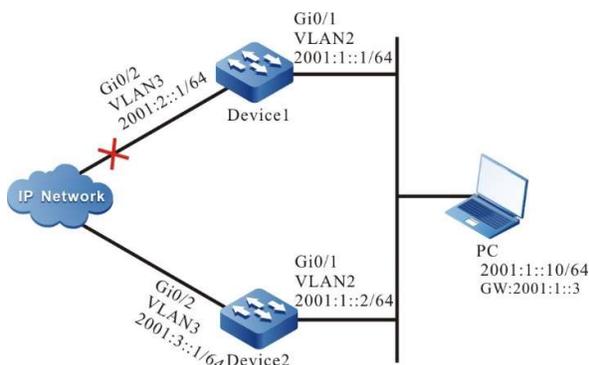


Figure 104-4 Network Topology for Configuring IPv6-based Coordination of VRRP with Track

#### Configuration Steps

Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configure the IPv6 address of each interface, and turn on the switch of RA response and RA period sending.

```
Device1#configure terminal
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ipv6 address fe80::1 link-local
Device1(config-if-vlan2)#ipv6 address 2001:1::1/64
Device1(config-if-vlan2)#no ipv6 nd suppress-ra period
Device1(config-if-vlan2)#no ipv6 nd suppress-ra response
Device1(config-if-vlan2)#exit
Device2#configure terminal
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ipv6 address fe80::2 link-local
Device2(config-if-vlan2)#ipv6 address 2001:1::2/64
Device2(config-if-vlan2)#no ipv6 nd suppress-ra period
Device2(config-if-vlan2)#no ipv6 nd suppress-ra response
Device2(config-if-vlan2)#exit
```

Step 3: Create an IPv6-based VRRP group.

#On Device1, configure VRRP group 1, with virtual IP address of 2001:1::3 and fe80::100 and priority configured of 110.

```
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ipv6 vrrp 1 ip fe80::100 link-local
Device1(config-if-vlan2)#ipv6 vrrp 1 ip 2001:1::3
Device1(config-if-vlan2)#ipv6 vrrp 1 priority 110
Device1(config-if-vlan2)#exit
```

#On Device2, configure VRRP group 1, with virtual IP address of 2001:1::3 and fe80::100.

```
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ipv6 vrrp 1 ip fe80::100 link-local
Device2(config-if-vlan2)#ipv6 vrrp 1 ip 2001:1::3
Device2(config-if-vlan2)#exit
```

#View IPv6 VRRP status on Device1.

```
Device1# show ipv6 vrrp
Interface vlan2 (Flags 0x9)
  Pri-addr : fe80::1
  Vrf : 0
  Pri-matchaddr : fe80::1
  Virtual router : 1
  Mac mode: real mac mode
  Virtual IP address : fe80::100
  Global address count:1
    Global Match address : 2001:1::1
    Global Virtual IP address : 2001:1::3
  Virtual MAC address : 00-00-5e-00-02-01
  State : Master
  Normal priority : 110
  Current priority : 110
  Priority reduced : 0
  Preempt-mode : YES
  Advertise-interval : 100
  Authentication Mode : None
```

#View IPv6 VRRP status on Device2.

```
Device2#show ipv6 vrrp
Interface vlan2 (Flags 0x9)
  Pri-addr : fe80::2
  Vrf : 0
```

```

Pri-matchaddr : fe80::2
Virtual router : 1
Mac mode: real mac mode
Virtual IP address : fe80::100
Global address count:1
  Global Match address : 2001:1::2
  Global Virtual IP address : 2001:1::3
Virtual MAC address : 00-00-5e-00-02-01
State : Backup
Master addr : fe80::1
Normal priority : 100
Current priority : 100
Priority reduced : 0
Preempt-mode : YES
Advertise-interval : 100
Authentication Mode : None

```

Step 4: Configure coordination of VRRP with Track.

#On Device1, configure coordination of VRRPv3 with Track to monitor the uplink interface VLAN3, and configure the priority decrement as 20.

```

Device1#configure terminal
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ipv6 vrrp 1 track vlan3 20
Device1(config-if-vlan2)#exit

```

#View IPv6 VRRP status on Device1.

```

Device1#show ipv6 vrrp
Interface vlan2 (Flags 0x9)
Pri-addr : fe80::1
Vrf : 0
Pri-matchaddr : fe80::1
Virtual router : 1
Mac mode: real mac mode
Virtual IP address : fe80::100
Global address count:1
  Global Match address : 2001:1::1
  Global Virtual IP address : 2001:1::3
Virtual MAC address : 00-00-5e-00-02-01
State : Master
Normal priority : 110
Current priority : 110
Priority reduced : 0
Preempt-mode : YES
Advertise-interval : 100
Authentication Mode : None
Track interface : vlan3
Reduce : 20
Reduce state : NO

```

Step 5: Check the result.

When the monitoring interface VLAN3 of Device1 becomes down, VRRP priority decreases by 20. As a result, Device2 has a higher priority and switches to Master.

#View IPv6 VRRP status on Device1.

```

Device1#show ipv6 vrrp
Interface vlan2 (Flags 0x9)
Pri-addr : fe80::1
Vrf : 0
Pri-matchaddr : fe80::1
Virtual router : 1
Mac mode: real mac mode
Virtual IP address : fe80::100

```

```

Global address count:1
  Global Match address : 2001:1::1
  Global Virtual IP address : 2001:1::3
Virtual MAC address : 00-00-5e-00-02-01
State : Backup
Master addr : fe80::2
Normal priority : 110
Current priority : 90
Priority reduced : 20
Preempt-mode : YES
Advertise-interval : 100
Authentication Mode : None
Track interface : vlan3
Reduce : 20
Reduce state : YES

```

#View IPv6 VRRP status on Device2.

```

Device2#show ipv6 vrrp
Interface vlan2 (Flags 0x9)
Pri-addr : fe80::2
Vrf : 0
Pri-matchaddr : fe80::2
Virtual router : 1
Mac mode: real mac mode
Virtual IP address : fe80::100
Global address count:1
  Global Match address : 2001:1::2
  Global Virtual IP address : 2001:1::3
Virtual MAC address : 00-00-5e-00-02-01
State : Master
Normal priority : 100
Current priority : 100
Priority reduced : 0
Preempt-mode : YES
Advertise-interval : 100
Authentication Mode : None

```

### 104.3.3 Configure IPv6-based VRRP load Balancing

#### Network Requirements

- Create two IPv6-based VRRP backup groups on Device1 and Device2 which belong to two different VRRP groups. In particular, Device1 is a Master in group 1 and a Backup in group 2; Device2 is a Backup in group 1 and a Master in group 2.
- PC1 forwards data through Device1, and PC2 does so through Device2 to realize load balancing.

#### Network Topology

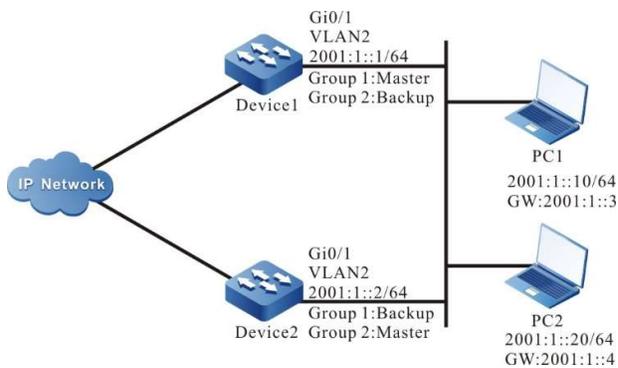


Figure 104-5 Network Topology for Configuring IPv6-based Load Balancing

### Configuration Steps

Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configure the IPv6 address of each interface, and turn on the switch of RA response and RA period sending.

```
Device1#configure terminal
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ipv6 address fe80::1 link-local
Device1(config-if-vlan2)#ipv6 address 2001:1::1/64
Device1(config-if-vlan2)#no ipv6 nd suppress-ra period
Device1(config-if-vlan2)#no ipv6 nd suppress-ra response
Device1(config-if-vlan2)#exit
Device2#configure terminal
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ipv6 address fe80::2 link-local
Device2(config-if-vlan2)#ipv6 address 2001:1::2/64
Device2(config-if-vlan2)#no ipv6 nd suppress-ra period
Device2(config-if-vlan2)#no ipv6 nd suppress-ra respons
Device2(config-if-vlan2)#exit
```

Step 3: Create IPv6-based VRRP group 1.

#On Device1, configure VRRP group 1, with virtual IP address of 2001:1::3 and fe80::100 and priority configured of 110.

```
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ipv6 vrrp 1 ip fe80::100 link-local
Device1(config-if-vlan2)#ipv6 vrrp 1 ip 2001:1::3
Device1(config-if-vlan2)#ipv6 vrrp 1 priority 110
Device1(config-if-vlan2)#exit
```

#On Device2, configure VRRP group 1, with virtual IP address of 2001:1::3 and fe80::100.

```
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ipv6 vrrp 1 ip fe80::100 link-local
Device2(config-if-vlan2)#ipv6 vrrp 1 ip 2001:1::3
Device2(config-if-vlan2)#exit
```

Step 4: Create IPv6-based VRRP group 2.

#On Device1, configure VRRP group 2, with the virtual IP address of 2001:1::4 and fe80::200.

```
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ipv6 vrrp 2 ip fe80::200 link-local
Device1(config-if-vlan2)#ipv6 vrrp 2 ip 2001:1::4
Device1(config-if-vlan2)#exit
```

#On Device2, configure VRRP group 2, with virtual IP address of 2001:1::4 and fe80::200 and priority configured of 110.

```
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ipv6 vrrp 2 ip fe80::200 link-local
Device2(config-if-vlan2)#ipv6 vrrp 2 ip 2001:1::4
Device2(config-if-vlan2)#ipv6 vrrp 2 priority 110
Device2(config-if-vlan2)#exit
```

Step 5: Check the result.

#On Device1, view IPv6 VRRP status in group 1 and 2.

```
Device1#show ipv6 vrrp
Interface vlan2 (Flags 0x9)
Pri-addr : fe80::1
Vrf : 0
Pri-matchaddr : fe80::1
Virtual router : 1
Mac mode: real mac mode
Virtual IP address : fe80::100
Global address count:1
  Global Match address : 2001:1::1
  Global Virtual IP address : 2001:1::3
Virtual MAC address : 00-00-5e-00-02-01
State : Master
Normal priority : 110
Currnet priority : 110
Priority reduced : 0
Preempt-mode : YES
Advertise-interval : 100
Authentication Mode : None

Pri-matchaddr : fe80::1
Virtual router : 2
Mac mode: real mac mode
Virtual IP address : fe80::200
Global address count:1
  Global Match address : 2001:1::1
  Global Virtual IP address : 2001:1::4
Virtual MAC address : 00-00-5e-00-02-02
State : Backup
Master addr : fe80::2
Normal priority : 100
Currnet priority : 100
Priority reduced : 0
Preempt-mode : YES
Advertise-interval : 100
Authentication Mode : None
```

#On Device2, view IPv6 VRRP status in group 1 and 2.

```
Device2#show ipv6 vrrp
Interface vlan2 (Flags 0x9)
Pri-addr : fe80::2
Vrf : 0
Pri-matchaddr : fe80::2
Virtual router : 1
Mac mode: real mac mode
Virtual IP address : fe80::100
Global address count:1
  Global Match address : 2001:1::2
  Global Virtual IP address : 2001:1::3
Virtual MAC address : 00-00-5e-00-02-01
State : Backup
Master addr : fe80::1
Normal priority : 100
Currnet priority : 100
Priority reduced : 0
Preempt-mode : YES
Advertise-interval : 100
Authentication Mode : None

Pri-matchaddr : fe80::2
Virtual router : 2
Mac mode: real mac mode
Virtual IP address : fe80::200
Global address count:1
```

Global Match address : 2001:1::2  
Global Virtual IP address : 2001:1::4  
Virtual MAC address : 00-00-5e-00-02-02  
State : Master  
Normal priority : 110  
Current priority : 110  
Priority reduced : 0  
Preempt-mode : YES  
Advertise-interval : 100  
Authentication Mode : None

It can be seen that as a Master of VRRP group 1, Device1 also acts as a Backup in VRRP group 2; as a Master of VRRP group 2, Device2 also acts as a Backup in VRRP group 1. When a device fails, the two PCs forward data through the other one. This can achieve both load balancing and mutual backup.





# 105 VBRP

---

## 105.1 Overview

VBRP (Virtual Backup Router Protocol) provides a backup function for gateway. It is used by multiple devices to maintain the uninterrupted forwarding of virtual gateway. VBRP maps multiple devices involved into a virtual router, and ensures that there is only one device which is forwarding packets on behalf of the virtual router. When the device responsible for forwarding task fails to work normally for some reason, another backup device will forward packets on behalf of the virtual router, and the device which cannot work normally will no longer undertake the forwarding task. This switching process is so short that it is transparent for the host in the LAN. As a result, you can reach the purpose of gateway backup.

The master and backup devices are hereinafter referred to as "Active" and "Standby" respectively.

## 105.2 VBRP Function Configuration

Table 105 VBRP Function Configuration List

Configuration Task	
Configure Basic Mode of VBRP	Enable VBRP Protocol
	Configure VBRP Priority
	Configure VBRP Preemption Mode
	Configure Real MAC Address of VBRP
Configure VBRP Network Authentication	Configure Simple Text Authentication of VBRP
	Configure VBRP MD5 Authentication
	Configure Coordination of VBRP with Track to Associate Uplink Interface

Configuration Task	
Configure Coordination of VBRP with Track to Associate Uplink Interface	Configure Coordination of VBRP with Track to Associate MLAG Role

### 105.2.1 Configure Basic Functions of VBRP

In various configuration tasks of VBRP, you must enable VBRP function first. Other functional performance configured cannot take effect until the virtual IP address of VBRP group is in the same network segment with interface IP address.

#### Configuration Condition

Before configuring basic functions of VBRP, do the following:

- Configure interface IP address.

#### Enable VBRP Protocol

To enable the VBRP function, you need to create a VBRP group under the interface and add the VBRP device to this group.

Table 105 Enabling VBRP Protocol

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	Mandatory
Configure VBRP group	<b>standby</b> [ <i>group-number</i> ] <b>ip</b> [ <i>ip-address</i> ]	Mandatory  Configure to add the device to the VBRP group. The <i>group-number</i> is 0 by default, and <i>ip-address</i> is a virtual IP address.

#### Configure VBRP Priority

After VBRP is configured, if no priority is set, the default priority 100 will be used; the device with a higher priority will be elected as the Active responsible for forwarding packets, and others will become Standbys; if all devices have the same priority, the election will be conducted according to the size of the interface IP

address of each device, and the device with a larger interface IP address becomes the Active. You can set the priority of VBRP as needed. The larger the value, the higher the priority.

Table 1 Configuring VBRP Priority

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	Mandatory
Configure the priority of VBRP group	<b>standby</b> [ <i>group-number</i> ] <b>priority</b> <i>value</i>	Mandatory Configure priority for this VRRP. The default priority is 100.

### Configure VBRP Preemption Mode

In preemption mode, once other devices in VBRP group finds their priority is higher than that of current Active, they will become the Active; in non-preemption mode, if the Active doesn't fail, other devices cannot become an Active even if they are configured with higher priority.

Table 2 Configuring VBRP Preemption Mode

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	Mandatory
Configure VBRP group as preemption mode	<b>standby</b> [ <i>group-number</i> ] <b>preempt</b> [ <i>delay delay-time</i> ]	Mandatory Configure this VBRP as preemption mode. By default, it is in non-preemption mode.

### Configure Real MAC Address of VBRP

After VBRP is configured, if the VBRP group should use real MAC address, the following command should be used for configuration. When the virtual router responds to an ARP request, it provides a real MAC address instead of a virtual MAC address. It is noteworthy that virtual MAC address is used by default.

Table 3 Configuring Real MAC Address of VBRP

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	Mandatory
Configure VBRP with real MAC address	<b>standby</b> [ <i>group-number</i> ] <b>use-bia</b>	Mandatory By default, virtual MAC address is used.

---

### Note

- By default, virtual MAC address is used after VBRP configuration is done. When the command **standby use-bia** is configured, real MAC address is used by the host to forward packets; after the command **no standby use-bia** is used, the virtual MAC address of corresponding interface is used by the host to forward packets.
- 

## 105.2.2 Configure VBRP Network Authentication

There are two types of authentication for VBRP, i.e. simple text authentication and MD5 authentication. For simple text authentication, there should be no more than 8 characters; for MD5 authentication, no more than 64 characters are required.

### Configuration Condition

Before configuring basic functions of VBRP, do the following:

- Configure VBRP group.

### Configure Simple Text Authentication of VBRP

Check and verify the effectiveness of VBRP packets by configuring VBRP authentication. VBRP simple text authentication can be configured with the following command.

Table 4 Configuring VBRP Simple Text Authentication

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	Mandatory
Configure Simple Text Authentication of VBRP	<b>standby</b> <i>group-number</i> <b>authentication</b> { <i>string</i> }	Mandatory  The authentication key configured is a string of no more than 8 characters.  By default, simple text authentication is disabled.

### Configure VBRP MD5 Authentication

Check and verify the effectiveness of VBRP packets by configuring VBRP authentication. VBRP MD5 authentication can be configured with the following command.

Table 5 Configuring VBRP MD5 Authentication

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	Mandatory
Configure VBRP MD5 Authentication	<b>standby</b> <i>group-number</i> <b>authentication</b> { <b>md5</b> { <b>key-id</b> <i>key-identifier</i> <b>key-string</b> <i>key-string</i> }   { <b>key-string</b> <i>key-string</i> } }	Mandatory  MD5 network authentication is configured, with a length of no more than 8 characters.  By default, MD5 authentication is disabled.

### 105.2.3 Configure Coordination of VBRP with Track

Associate VBRP with the uplink interface to be cared about through Track. When the uplink interface is down, the Active will automatically lower its priority and the Standby will receive the packet with a low priority and switch to Active. For details, see the figure below.

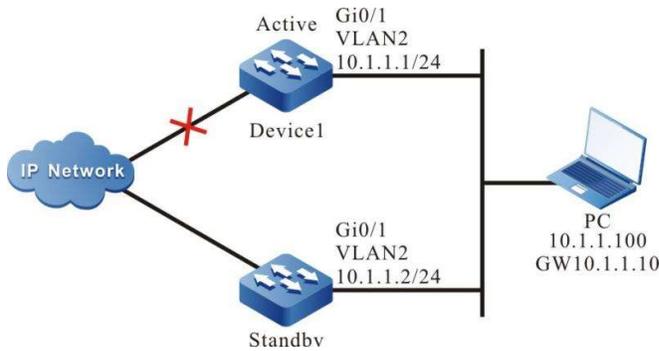


Figure 105 Configuring Coordination of VBRP with Track to Monitor Uplink of Active

#### Configuration Condition

Before configuring basic functions of VBRP, do the following:

- Configure VBRP group.

#### Configure Coordination of VBRP with Track to Associate Uplink Interface

Associate VBRP with the uplink interface to be cared about through Track. When the uplink interface is down, the Active will automatically lower its priority and the Standby will receive the VBRP packet with a low priority and switch to Active.

Table 6 Configuring Coordination of VBRP with Track to Associate with Uplink Interface

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	Mandatory
Configure coordination of VBRP with Track to associate uplink interface	<b>standby</b> [ <i>group-number</i> ] <b>track</b> { { <i>interface-name</i> }   <i>track-id</i> } [ <i>decrement</i> ]	Mandatory Configure the associated interface <i>interface-name</i> . When this interface becomes <i>down</i> , the <i>decrement</i> of its priority decreases by 10 by default.

### Configure Coordination of VBRP with Track to Associate BFD and RTR

If Track is associated with BFD and RTR, the Active can directly associate with this Track group to monitor the lines. When any failure occurs on the lines, the Active decreases its priority. At this moment, the Standby switches to Active after receiving the VBRP packet with a low priority.

Table 7 Configuring Coordination of VBRP with Track to Associate with BFD and RTR

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	Mandatory
Configure coordination of VBRP with Track to associate uplink interface	<b>standby</b> [ <i>group-number</i> ] <b>track</b> { <i>track-id</i> } [ <i>decrement</i> ]	Mandatory Configure the associated Track <i>track-id</i> and associate this Track with BFD and RTR; by default, the priority decreases by 10.

---

#### Note

- For the configurations of associating Track with BFD and RTR, see Track-related chapter in the User Manual.
- 

### Configure Coordination of VBRP with Track to Associate MLAG Role

After configuration, the MLAG active device can perform protocol interaction; the MLAG standby device which maintains at standby doesn't perform protocol interaction.

Table 8 Configuring Coordination of VBRP with Track to Associate MLAG Role

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	Mandatory
Configure coordination of VBRP with Track to associate uplink interface	<b>standby</b> [ <i>group-number</i> ] <b>track mlag role</b>	Mandatory  Configure the associated MLAG role.  In particular, group-number is the VBRP group number.

## 105.2.4 VBRP Monitoring and Maintaining

Table 9 VBRP Monitoring and Maintaining

Command	Description
<b>Show standby</b> [brief]   [ all ]   [ interface <i>interface-name</i> group gid]	Show the VBRP configuration information, including virtual IP address, virtual MAC address, device status, device priority, and dependent device interface address.

## 105.3 Typical Configuration Example of VBRP

### 105.3.1 Configure Basic Mode of VBRP

#### Network Requirements

- Enable VBRP between Device1 and Device2 so that Device1 and Device2 can share a virtual IP address to back up the default gateway of the user's host, reducing the time of network disconnection.

#### Network Topology

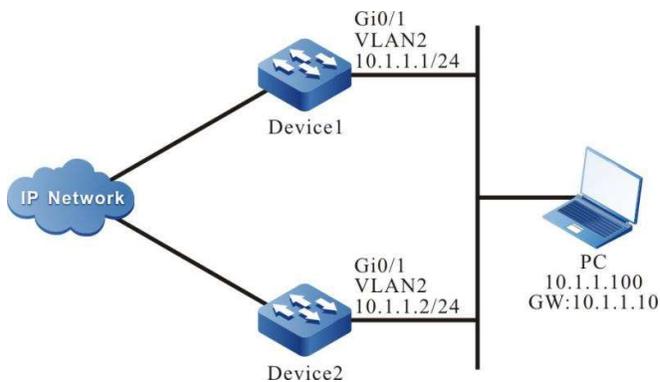


Figure 105 Network Topology for Configuring Basic Mode of VBRP

### Configuration Steps

Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configure IP addresses for the ports. (Omitted)

Step 3: Create VBRP group.

#On Device1, configure VBRP group 1, with virtual IP address of 10.1.1.10; enable the preemption function; configure priority as 110.

```
Device1#configure terminal
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#standby 1 ip 10.1.1.10
Device1(config-if-vlan2)#standby 1 preempt
Device1(config-if-vlan2)#standby 1 priority 110
```

#On Device2, configure VBRP group 1, with virtual IP address of 10.1.1.10, and enable the preemption function.

```
Device2#configure terminal
Device1(config-if-vlan2)#standby 1 ip 10.1.1.10
Device1(config-if-vlan2)#standby 1 preempt
Device1(config-if-vlan2)#standby 1 priority 110
```

Step 4: Check the result.

#View the VBRP status of Device1.

```
Device1#show standby
Interface vlan2
  Primary address 10.1.1.1, state up
  Group 1
  State is Active
  Virtual IP address is 10.1.1.10
  Refer to local IP prefix 193.168.1.1/24
  Local virtual MAC address is 0000.0c07.ac01
  Current MAC type VMAC, installed into HW
  Hello time 3 sec, hold time 10 sec
  Next hello sent in 0.633348 secs
  Preemption enabled, delay 0 sec
```

```
Active router is local
Standby router is 10.1.1.2,priority 100 (expires in 8.466648 secs)
Priority 110 (configured 110)
```

#View the VBRP status of Device2.

```
Device2#show standby
Interface vlan2
  Primary address 10.1.1.2, state up
  Group 1
  State is Standby
  Virtual IP address is 10.1.1.10
  Refer to local IP prefix 10.1.1.2/24
  Local virtual MAC address is 0000.0c07.ac01
  Current MAC type VMAC
  Hello time 3 sec, hold time 10 sec
  Next hello sent in 0.450022 secs
  Preemption enabled, delay 0 sec
  Active router is 10.1.1.1, priority 110 (expires in 7.266656 secs)
  Standby router is local
  Priority 100 (configured 100)
```

It can be seen from the VBRP status that Device1, in Active status, has a VBRP priority of 110, and Device2 has a VBRP status of Standby. When Device1 fails, Device2 automatically switches to Active for data forwarding.

---

## Note

- For VBRP status, the device with a higher priority is the Active. When they have the same priority, the device with a larger interface IP address is the Active.
  - By default, VBRP works in the non-preemption mode. Preemption mode which needs to be configured manually is recommended.
  - By default, the default VBRP priority is 100.
- 

## 105.3.2 Configure Coordination of VBRP with Track

### Network Requirements

- Enable VBRP between Device1 and Device2.
- Device1 monitors the status of VLAN3 through Track. When the uplink interface VLAN3 of Device1 is down, VBRP can sense and switch status so that the Standby will become an Active for data forwarding.

### Network Topology

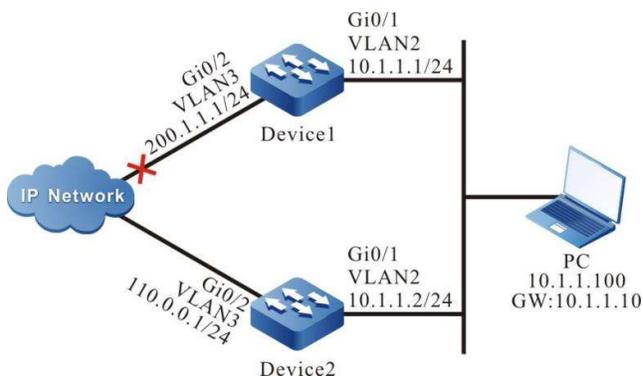


Figure 1 Network Topology for Coordination of VBRP with Track

### Configuration Steps

Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configure IP addresses for the ports. (Omitted)

Step 3: Create VBRP group.

#On Device1, configure VBRP group 1 with virtual IP address of 10.1.1.10; enable the preemption function; configure priority as 110.

```
Device1#configure terminal
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#standby 1 ip 10.1.1.10
Device1(config-if-vlan2)#standby 1 preempt
Device1(config-if-vlan2)#standby 1 priority 110
```

#On Device2, configure VBRP group 1 with virtual IP address of 10.1.1.10, and enable the preemption function.

```
Device2#configure terminal
Device2(config)#interface vlan 2
Device2(config-if-vlan2)#standby 1 ip 10.1.1.10
Device2(config-if-vlan2)#standby 1 preempt
```

#View the VBRP status of Device1.

```
Device1#show standby
Interface vlan2
  Primary address 10.1.1.1, state up
Group 1
  State is Active
  Virtual IP address is 10.1.1.10
  Refer to local IP prefix 10.1.1.1/24
  Local virtual MAC address is 0000.0c07.ac01
  Current MAC type VMAC, installed into HW
  Hello time 3 sec, hold time 10 sec
  Next hello sent in 0.533352 secs
  Preemption enabled, delay 0 sec
  Active router is local
  Standby router is 10.1.1.2, priority 100 (expires in 9.283362 secs)
  Priority 110 (configured 110)
```

#View the VBRP status of Device2.

```
Device2#show standby
Interface vlan2
  Primary address 10.1.1.2, state up
Group 1
  State is Standby
  Virtual IP address is 10.1.1.10
  Refer to local IP prefix 10.1.1.2/24
  Local virtual MAC address is 0000.0c07.ac01
  Current MAC type VMAC
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.516646 secs
  Preemption enabled, delay 0 sec
  Active router is 10.1.1.1, priority 110 (expires in 9.516646 secs)
  Standby router is local
  Priority 100 (configured 100)
```

Step 4: Configure coordination of VBRP with Track.

#On Device1, configure coordination of VBRP with Track to monitor the uplink interface VLAN3, and configure the priority decrement as 20.

```
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#standby 1 track vlan 3 20
```

#View the VBRP status of Device1.

```
Device1#show standby
Interface vlan2
  Primary address 10.1.1.1, state up
Group 1
  State is Active
  Virtual IP address is 10.1.1.10
  Refer to local IP prefix 10.1.1.1/24
  Local virtual MAC address is 0000.0c07.ac01
  Current MAC type VMAC, installed into HW
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.533352 secs
  Preemption enabled, delay 0 sec
  Active router is local
  Standby router is 10.1.1.2, priority 100 (expires in 9.283362 secs)
  Priority 110 (configured 110)
  Track interface vlan3 state Up decrement 20
```

#When the uplink interface VLAN3 of Device1 is down, VBRP priority decreases by 20. As a result, Device2 has a higher priority, which causes status switch.

#View the VBRP status of Device1.

```
Device1#show standby
Interface vlan2
  Primary address 10.1.1.1, state up
Group 1
  State is Standby
  Virtual IP address is 10.1.1.10
  Refer to local IP prefix 10.1.1.1/24
  Local virtual MAC address is 0000.0c07.ac01
  Current MAC type VMAC
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.800008 secs
  Preemption enabled, delay 0 sec
  Active router is 10.1.1.2, priority 100 (expires in 7.766676 secs)
```

```
Standby router is local
Priority 90 (configured 110)
Track interface vlan3 state Down decrement 20
```

#View the VBRP status of Device2.

```
Device2#show standby
Interface vlan2
  Primary address 10.1.1.2, state up
Group 1
  State is Active
  Virtual IP address is 10.1.1.10
  Refer to local IP prefix 10.1.1.2/24
  Local virtual MAC address is 0000.0c07.ac01
  Current MAC type VMAC, installed into HW
  Hello time 3 sec, hold time 10 sec
  Next hello sent in 0.533352 secs
  Preemption enabled, delay 0 sec
  Active router is local
  Standby router is 10.1.1.1, priority 90 (expires in 9.283362 secs)
  Priority 100 (configured 100)
```

### 105.3.3 Configure VBRP load Balancing Mode

#### Network Requirements

- Device1 and Device2 belong to two different VBRP groups. In particular, Device1 is an Active in group 1 and a Standby in group 2; Device2 is a Standby in group 1 and an Active in group 2.
- PC1 forwards data through Device1, and PC2 does so through Device2 to realize load balancing.

#### Network Topology

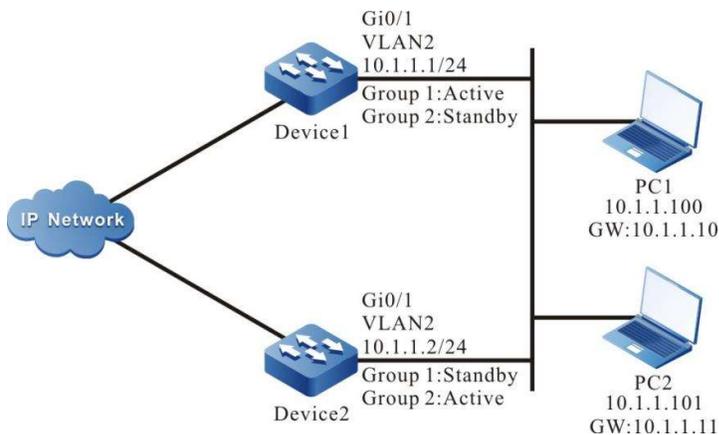


Figure 2 Network Topology for VBRP Load Balancing

#### Configuration Steps

Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configure IP addresses for the ports. (Omitted)

Step 3: Create VBRP group 1.

#On Device1, configure VBRP group 1 with virtual IP address of 10.1.1.10; enable the preemption function; configure priority as 110.

```
Device1#configure terminal
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#standby 1 ip 10.1.1.10
Device1(config-if-vlan2)#standby 1 preempt
Device1(config-if-vlan2)#standby 1 priority 110
```

#On Device2, configure VBRP group 1 with virtual IP address of 10.1.1.10, and enable the preemption function.

```
Device2#configure terminal
Device2(config)#interface vlan 2
Device2(config-if-vlan2)#standby 1 ip 10.1.1.10
Device2(config-if-vlan2)#standby 1 preempt
```

Step 4: Create VBRP group 2.

#On Device1, configure VBRP group 2 with virtual IP address of 10.1.1.11, and enable the preemption function.

```
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#standby 2 ip 10.1.1.11
Device1(config-if-vlan2)#standby 2 preempt
```

#On Device2, configure VBRP group 1 with virtual IP address of 10.1.1.11; enable the preemption function; configure priority as 120.

```
Device2(config)#interface vlan 2
Device2(config-if-vlan2)#standby 2 ip 10.1.1.11
Device2(config-if-vlan2)#standby 2 preempt
Device2(config-if-vlan2)#standby 2 priority 120
```

Step 5: Check the result.

#On Device1, view VBRP status in group 1 and 2.

```
Device1#show standby
Interface vlan2
  Primary address 10.1.1.1, state up
  Group 1
  State is Active
  Virtual IP address is 10.1.1.10
  Refer to local IP prefix 10.1.1.1/24
  Local virtual MAC address is 0000.0c07.ac01
  Current MAC type VMAC, installed into HW
  Hello time 3 sec, hold time 10 sec
  Next hello sent in 0.633348 secs
  Preemption enabled, delay 0 sec
  Active router is local
  Standby router is 10.1.1.2, priority 100 (expires in 7.83370 secs)
```

```
Priority 110 (configured 110)
Group 2
State is Standby
Virtual IP address is 10.1.1.11
Refer to local IP prefix 10.1.1.1/24
Local virtual MAC address is 0000.0c07.ac02
Current MAC type VMAC
Hello time 3 sec, hold time 10 sec
  Next hello sent in 0.950002 secs
Preemption enabled, delay 0 sec
Active router is 10.1.1.2, priority 120 (expires in 7.300028 secs)
Standby router is local
Priority 100 (configured 100)
```

#On Device2, view VBRP status in group 1 and 2.

```
Device2#show standby
Interface vlan2
Primary address 10.1.1.2, state up
Group 1
State is Standby
Virtual IP address is 10.1.1.10
Refer to local IP prefix 10.1.1.2/24
Local virtual MAC address is 0000.0c07.ac01
Current MAC type VMAC
Hello time 3 sec, hold time 10 sec
  Next hello sent in 0.600016 secs
Preemption enabled, delay 0 sec
Active router is 10.1.1.1, priority 110 (expires in 7.700012 secs)
Standby router is local
Priority 100 (configured 100)
Group 2
State is Active
Virtual IP address is 10.1.1.11
Refer to local IP prefix 10.1.1.2/24
Local virtual MAC address is 0000.0c07.ac02
Current MAC type VMAC, installed into HW
Hello time 3 sec, hold time 10 sec
  Next hello sent in 0.816674 secs
Preemption enabled, delay 0 sec
Active router is local
Standby router is 10.1.1.1, priority 100 (expires in 8.33332 secs)
Priority 120 (configured 120)
```

It is indicated that as an Active of VBRP group 1, Device1 also acts as a Standby in VBRP group 2. On the contrary, as an Active of VBRP group 2, Device2 also acts as a Standby in VBRP group 2. When a device fails, the two PCs forward data through the other one. This can achieve both load balancing and mutual backup.

# 106 Load-Balance Virtual Router Redundancy Protocol

## 106.1 Overview

Load-Balance Virtual Router Redundancy Protocol (Load-Balance VRRP) is a routing protocol which allows dynamic load of clients configured with the same gateway when there are multiple gateway exits in the LAN. It also considers the redundant backup feature.

The master and backup devices are hereinafter referred to as "Master" and "Backup" respectively.

## 106.2 Load-Balance Virtual Router Redundancy Protocol Function Configuration

### Configuration

Table 106 Load-Balance VRRP Function Configuration List

Configuration Task	
Configure Current VRRP Mode	Enable Load-Balance VRRP Mode
Configure Basic Functions of Load-Balance VRRP	Enable Load-Balance VRRP
	Configure Priority for Load-Balance VRRP
	Configure Virtual MAC Address of Load-Balance VRRP
Configure Timer of Load-Balance VRRP	Configure Interval of HELLO Packet Period
	Configure Interval of Keep Packet Period
	Configure Dead Timer for Virtual MAC Address
	Configure Terminal Aging Timer on Forwarding Lane
	Configure Terminal Detection Timer on Forwarding Lane

## 106.2.1 Configure Current Mode of Load-Balance VRRP

Among various configuration tasks of Load-Balance VRRP, Load-Balance VRRP mode must be enabled first. This mode and VRRP standard protocol are mutually exclusive.

### Configuration Condition

None

### Enable Load-Balance VRRP Mode

Table 1 Enabling Load-Balance VRRP Mode

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>vrrp mode load-balance</b>	Mandatory

## 106.2.2 Configure Basic Functions of Load-Balance VRRP

Among various configuration tasks of VRRP, Load-Balance VRRP mode must be enabled first. Other functional performance configured cannot take effect until the virtual IP address of Load-Balance VRRP group is in the same network segment with the interface IP address.

### Configuration Condition

Before configuring the basic VRRP functions, do the following:

- Configure interface IP address.

### Enable Load-Balance VRRP

To enable the Load-Balance VRRP function, you are required to create a Load-Balance VRRP group under the interface and configure virtual IP address.

Table 106 Enabling VRRP

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface <i>interface-name</i></b>	Mandatory

Step	Command	Description
Configure Load-Balance VRRP group	<b>vrrp vrid ip ip-address</b>	Mandatory  Enable Load-Balance VRRP. In particular, vrid is the Load-Balance VRRP group number, and ip-address is the virtual IP address.

---

## Note

- In the Load-Balance VRRP mode, the virtual IP shall not be the same as the interface IP.
- 

### Configure Priority for Load-Balance VRRP

After Load-Balance VRRP is configured, if no priority is set, the default priority 100 will be used; the device with a higher priority will be elected as the Master responsible for forwarding packets, and others will become Backups; if all devices have the same priority, the election will be conducted according to the size of the interface IP address of each device, and the device with a larger interface IP address becomes the Master. You can set the priority of Load-Balance VRRP as needed. The larger the value, the higher the priority.

Table 2 Configuring Load-Balance VRRP Priority

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface interface-name</b>	Mandatory
Configure the priority of Load-Balance VRRP group	<b>vrrp vrid priority priority</b>	Mandatory  Configure Load-Balance VRRP priority. The default priority is 100.

### Configure Simple Text Authentication of Load-Balance VRRP

After the Load-Balance VRRP is configured, if not set, simple text authentication is disabled by default; neighbors cannot be successfully established or negotiate unless the authentications in the Load-Balance VRRP group are consistent.

Table 106-5 Configuring Simple Text Authentication of Load-Balance VRRP

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	Mandatory
Configure simple text authentication of Load-Balance VRRP	<b>vrrp vrid authentication text</b> <i>string</i>	Mandatory  By default, the simple text authentication function is disabled.  The authentication key should have no more than 8 characters.

### Configure Real MAC Address of Load-Balance VRRP

Each virtual router in a Load-Balance VRRP has one virtual MAC address. According to the provisions of Load-Balance VRRP, the format of the virtual MAC address is as follows: 00.01.7a.00.{vrid}.{mid}. The mid value is assigned by the master. When the virtual router responds to an ARP request, it provides a virtual MAC address instead of a real MAC address of the interface. It is noteworthy that virtual MAC address is used by default.

Table 3 Configuring Real MAC Address of Load-Balance VRRP

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	Mandatory
Configure real MAC address for Load-Balance VRRP	<b>vrrp vrid use-bia</b>	Mandatory  By default, virtual MAC address is used.

---

 **Note**

- By default, virtual MAC address is used after VRRP configuration. When the commands mentioned in this section are configured, the real MAC address on corresponding interface is used by the host to forward packets; after deleting these commands, the virtual MAC address of corresponding interface is used by the host to forward packets.
- 

### 106.2.3 Configure Timer of Load-Balance VRRP

In Load-Balance VRRP, perform corresponding actions according to corresponding timer so as to maintain relevant status.

#### Configuration Condition

Before configuring Load-Balance VRRP timer, do the following:

- Switch current VRRP mode to Load-Balance VRRP mode
- Enable this Load-Balance VRRP group

#### Configure Interval of HELLO Packet Period

Hello packet is responsible for advertising some of its information to its neighbors and maintaining neighbor relation. Therefore, the neighbors within the same group should have consistent sending periods of Hello packets.

Table 4 Configuring Interval of Hello Packet Sending Period

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	Mandatory
Configure interval of Hello packet sending period of Load-Balance VRRP group	<b>vrrp vrid timers hello</b> <i>Hello-time</i> [ <b>hold</b> <i>Hold-time</i> [ <b>preserved</b> <i>Preserved-time</i> [ <b>delay-vote</b> <i>Delay-vote-time</i> ] ] ]	Mandatory Configure interval of Hello packet sending period. In particular, vrid is VRRP group number, and Hello-time specifies the sending period of Hello packet in VRRP group.

Step	Command	Description
		Hold-time specifies the hold time of neighbors in VRRP group. Preserved-time specifies the hold time of virtual MAC in VRRP group. Delay-vote-time specifies the time of voting delay in group.

### Configure Interval of Keep Packet Period

Keep packet is mainly responsible for advertising the virtual mac address of this virtual router to layer-2 switch to refresh the layer-2 MAC entries of the switch for traffic redirection.

Table 5 Configuring Interval of Keep Packet Sending Period

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	Mandatory
Configure interval of Keep packet sending period of Load-Balance VRRP group	<b>vrrp vrid timers keep</b> <i>keep-time</i>	Mandatory  Configure interval of Keep packet sending period. In particular, vrid is Load-Balance VRRP group number, and Keep-time specifies the sending period of Keep packet of Load-Balance VRRP group.

### Configure Dead Timer for Virtual MAC Address

After the owner fails, the virtual mac will experience the hold state and reach the dead state. The time of the dead state configured should be greater than the ARP aging time of the underlying terminal.

Table 6 Configuring Dead Timer of Virtual MAC Address

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	Mandatory
Configure dead time for virtual MAC address of Load-Balance VRRP group	<b>vrp vrid timers zombie</b> <i>zombie-time</i>	Mandatory Configure Dead Timer for Virtual MAC Address In particular, vrid is Load-Balance VRRP group number, and Zombie-time specifies the dead time of virtual mac of Load-Balance VRRP group.

### Configure Terminal Aging Timer on Forwarding Lane

When managing the terminal in the forwarding layer, if this terminal is not online for a long time, it will be aged to release the resources occupied by this terminal. As a result, the terminal entries of this group will be refreshed.

Table 7 Configuring Terminal Aging Timer on Forwarding Lane

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	Mandatory
Configure terminal aging timer of Load-Balance VRRP group on forwarding lane	<b>vrp vrid timers forwarding ageing</b> <i>forwarding-ageing-time</i>	Mandatory Configure terminal aging timer on forwarding lane. In particular, vrid is VRRP group number, and forwarding-ageing-time specifies the terminal aging time on forwarding lane in VRRP group.

## Configure Terminal Detection Timer on Forwarding Lane

When managing the terminal on forwarding lane, the online status of this terminal will be periodically detected so as to update the status of this local terminal.

Table 8 Configuring Terminal Detection Timer on Forwarding Lane

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	Mandatory
Configure terminal detection timer of Load-Balance VRRP group on Forwarding Lane	<b>vrrp vrid timers forwarding dtct</b> <i>forwarding-dtct-time</i>	Mandatory Configure terminal detection timer on forwarding lane. In particular, vrid is the Load-Balance VRRP group number. Forwarding-dtct-time specifies the terminal detection time on forwarding lane in Load-Balance VRRP group.

## 106.2.4 Load-Balance VRRP Monitoring and Maintaining

Table 9 VRRP Monitoring and Maintaining

Command	Description
Show vrrp [ interface <i>interface-name</i> ]	Show the Load-Balance VRRP configuration information, including virtual IP address, virtual MAC address, device status, device priority, dependent device interface address, and coordination group.

## 106.3 Typical Configuration Example of Load-Balance VRRP

### 106.3.1 Configure Basic Functions of Load-Balance VRRP

#### Network Requirements

- On Device1 and Device2, create a Load-Balance VRRP backup group so that Device1 and Device2 can share a virtual IP address to back up the default gateway of the user's host, reducing the time of network disconnection.
- The Load-Balance VRRP implements load function by assigning the traffic of different users' host to different VRRP devices for forwarding within a group. Unlike common VRRP, the Backup devices in Load-Balance VRRP can also forward traffic so that users can configure the same gateway address for all the hosts in the network to implement the load balancing function.

#### Network Topology

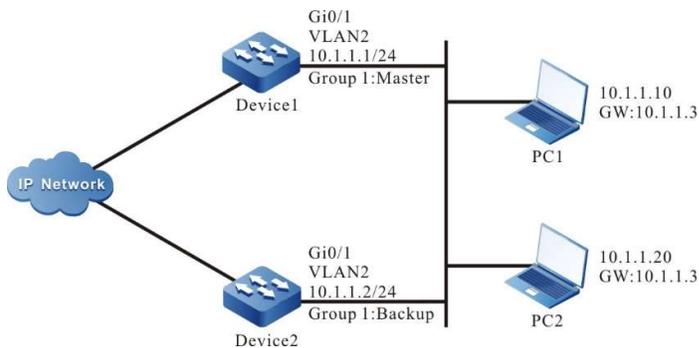


Figure 106 Network Topology for Configuring Basic Functions of Load-Balance VRRP

#### Configuration Steps

Step 1: Configure IPv4 addresses for the ports. (Omitted)

Step 2: Configure the device as Load-Balance VRRP mode.

#### #Configure Device1.

```
Device1#configure terminal
Device1(config)#vrrp mode load-balance
```

#### #Configure Device2.

```
Device2#configure terminal
Device2(config)#vrrp mode load-balance
```

#### #View the VRRP mode of Device1.

```
Device1#show vrrp-pub mode

Current mode:load_balance
Current switch:0
```

#View the VRRP mode of Device2.

```
Device2#show vrrp-pub mode

Current mode:load_balance
Current switch:0
```

It is indicated that both Device1 and Device2 are running Load-Balance VRRP mode.

Step 3: Create a Load-Balance VRRP backup group.

#On Device1, create backup group 1, with virtual IP address of 10.1.1.3 and priority configured of 110.

```
Device1(config)#interface vlan2
Device1(config-if-vlan2)#vrrp 1 ip 10.1.1.3
Device1(config-if- vlan2)#vrrp 1 priority 110
Device1(config-if- vlan2)#exit
```

#On Device2, create backup group 1, with virtual IP address of 10.1.1.3.

```
Device2(config)#interface vlan2
Device2(config-if-vlan2)#vrrp 1 ip 10.1.1.3
Device2(config-if- vlan2)#exit
```

Step 4: View the Load-Balance VRRP status.

#View the neighbor table of Load-Balance VRRP on Device1.

```
Device1#show vrrp neighbor

Gid Neighbor Priority Uid Virtual-ip Master Hold-time Interface
1 10.1.1.2 100 412780 10.1.1.3 10.1.1.1 36 vlan2
```

#It is indicated from the neighbor field that Device1 has successfully established neighbor relation with Device2.

#View the neighbor table of Load-Balance VRRP on Device2.

```
Device2#show vrrp neighbor

Gid Neighbor Priority Uid Virtual-ip Master Hold-time Interface
1 10.1.1.1 110 348619 10.1.1.3 10.1.1.1 33 vlan2
```

#It is indicated from the neighbor field that Device2 has successfully established neighbor relation with Device1.

#View the Load-Balance VRRP status of Device1.

```
Device1#show vrrp
Interface vlan2
Vrf:0
Virtual router : 1
Mac mode: virtual mac mode
Forwording mac :
00.01.7a.00.01.01 ,installed into HW
Virtual IP address : 10.1.1.3
Match address : 10.1.1.1
State : Master
Priority : 110
Hello interval(sec) : 10
next hello in 3 secs
Hold time(sec) : 40
```

```
Delay vote time(sec) : 40
Delay delete time(sec) : 20
Preserve time(sec) : 40
Keep(min) : 15
Zombie(min) : 10
Uid : 348619
Terminal number : 0/1000
```

It is indicated from the State field that Device1 has been elected as a Master.

#View the Load-Balance VRRP status of Device2.

```
Device2#show vrrp
Interface vlan2
Vrf:0
Virtual router : 1
  Mac mode: real mac mode
  Forwarding mac :
    00.01.7a.00.01.02 ,installed into HW
  Virtual IP address : 10.1.1.3
  Match address : 10.1.1.2
  State : Backup
  master:10.1.1.1
  Priority : 100
  Hello interval(sec) : 10
    next hello in 6 secs
  Hold time(sec) : 40
  Delay vote time(sec) : 40
  Delay delete time(sec) : 20
  Preserve time(sec) : 40
  Keep(min) : 15
  Zombie(min) : 10
  Uid : 412780
  Terminal number : 0
```

It is indicated from the State field that Device2 has become a Backup.

#View the MAC address forwarding allocation table of Load-Balance VRRP on Device1.

```
Device1# show vrrp fmac

Gid Virtual-ip Forwarding-mac Owner Backup Owner-state Timeout Interface
1 10.1.1.3 0001.7a00.0101 10.1.1.1 - Active - vlan2
1 10.1.1.3 0001.7a00.0102 10.1.1.2 - Active - vlan2
```

Only the Master have the MAC address forwarding allocation function. It is indicated from the corresponding relation between Owner and Forwarding-mac that the MAC forwarding address allocated to 10.1.1.1 is 0001.7a00.0101, and that allocated to 10.1.1.2 is 0001.7a00.0102.

---

## Note

- The Load-Balance VRRP can work in non-preemption mode only.
  - The Load-Balance VRRP enables election delay timer in init status, 4 times the hello interval by default. Elect after time-out.
  - The Load-Balance VRRP elects according to the priority. The device with a higher priority is the Master. When they have the same priority, the device with a larger interface IP address is the Master, and others become Backups.
-

Step 5: Check the result.

#Test the connectivity on PC1 and PC2 by pinging gateway. #View the gateway forwarding MAC address assigned by the Master to the host terminal on Device1.

```
Device1#show vrrp terminal
```

Gid	Virtual-ip	Terminal	Forwarding-mac	Interface
1	10.1.1.3	10.1.1.10	0001.7a00.0101	vlan2
1	10.1.1.3	10.1.1.20	0001.7a00.0102	vlan2

It can be seen from the table above that different gateway forwarding MAC addresses have been assigned to host terminals PC1 and PC2. Plus the MAC forwarding address assigned by the Master to Device1 and Device2 mentioned in step 4, you can see that the traffics of PC1 and PC2 are forwarded by Device1 and Device2 respectively for load balancing.

#View the MAC forwarding address allocation table for terminal gateway of Backup on Device2.

```
Device2#show vrrp terminal
```

Gid	Virtual-ip	Terminal	Forwarding-mac	Interface
1	10.1.1.3	10.1.1.10	0001.7a00.0101	vlan2
1	10.1.1.3	10.1.1.20	0001.7a00.0102	vlan2

The Master will synchronize the MAC forwarding address allocation table for terminal gateway to all VRRP devices.

# 107 Track

---

## 107.1 Overview

Track can be used to monitor some information when the system is operating. Other service modules can monitor the changes that occur during system operation by associating with Track. After the service module is associated with Track, when the information monitored by Track changes, Track will notify the service module which then process the changes accordingly. For example, in practical applications, VRRP and VBRP often monitor the status of uplink interface, network reachability and other information by associating with Track, and adjust their own priorities based on this information for the switch between active and standby devices.

## 107.2 Track Function Configuration

Table 107 Track Function Configuration List

Configuration Task	
Configure Track Group	Configure Track Group
Configure Monitoring Object	Configure Status of Monitoring Interface
	Configure Direct Route of Monitoring Interface
	Configure Bandwidth Utilization Rate Alarm in Incoming and Outgoing Directions of Monitoring Interface
	Configure Reachability of Monitoring Route
	Configure Status of Monitoring Aggregation Group
	Configure to Monitor Status of Layer-2 Ethernet Interface

Configuration Task	
	Configure Monitoring RTR Group
	Configure Monitoring BFD Session

### 107.2.1 Configure Track Group

#### Configuration Condition

None

#### Configure Track Group

The system can be configured with multiple Track groups that are independent of each other, and a Track group may contain multiple monitoring objects.

The Track group has two logics, i.e. "and" and "or":

- When the logic of Track group is "and", the status of Track group will become up only when all monitoring objects therein are in up status; otherwise, it will be in down status;
- When the logic of Track group is "or", the status of Track group will become up only if one monitoring object therein is in up status; otherwise, it will be in down status.

Table 107 Configuring Track Group

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Create a Track group	<b>track <i>group-id</i></b>	Mandatory
Configure the logic of Track group	<b>logic { operator [ AND   OR ]   reverse }</b>	Optional AND: Logical "and" OR: Logical "or" Reverse: Logical reverse  By default, the logic of Track group is "and"; the logical reverse function doesn't take effect.

---

 **Note**

- When the service module needs to monitor some information through Track, in addition to configuring monitoring object in the Track group, you are also required to refer to relevant chapter of each service module in the User Manual to configure the service module to associate with the Track group command.
- 

## 107.2.2 Configure Monitoring Object

### Configuration Condition

Before configuring monitoring object, do the following:

- Configure Track group.

### Configure Status of Monitoring Interface

The monitoring object to be configured in the Track group is interface status. When the network layer protocol of interface is up, the status of this monitoring object is up; when the network layer protocol of interface is down, the status of this monitoring object is down.

Table 1 Configuring to Monitor IPv4 Status of Interface

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the Track configuration mode	<b>track track-id</b>	-
Configure Status of Monitoring Interface	<b>interface interface-name</b> <b>line-protocol</b>	Mandatory

Table 2 Configuring to Monitor IPv6 Status of Interface

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the Track configuration mode	<b>track track-id</b>	-
Configure Status of Monitoring Interface	<b>interface interface-name</b> <b>line-ipv6-protocol</b>	Mandatory

### Configure Direct Route of Monitoring Interface

The monitoring object to be configured in the Track group is direct route of interface. When the interface has an IP address and its status is up, the status of the monitoring object is up; when the interface doesn't have any IP address or its status is down, the status of the monitoring object is down.

Table 107 Configuring to Monitor Direct IPv4 Route of Interface

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the Track configuration mode	<b>track track-id</b>	-
Configure Direct Route of Monitoring Interface	<b>interface interface-name</b> <b>ip-routing</b>	Mandatory

Table 3 Configuring to Monitor Direct IPv6 Route of Interface

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the Track configuration mode	<b>track track-id</b>	-
Configure Direct Route of Monitoring Interface	<b>interface interface-name</b> <b>ipv6-routing</b>	Mandatory

### Configure to Monitor Bandwidth Utilization Rate Alarm of Interface

In the Track group, the monitoring object can be configured with bandwidth utilization rate alarm in incoming and outgoing directions of interface. When the incoming traffic of an interface is higher than the bandwidth utilization rate alarm value in the incoming direction set for the interface, the status of the monitoring object is up; when the incoming traffic of the interface is lower than the bandwidth utilization alarm value in the incoming direction set for the interface, the status of the monitoring object is down; when the outgoing traffic of the interface is higher than the bandwidth utilization value in the outgoing direction set for the interface, the status of the monitoring object is up; when the outgoing traffic of the interface is lower than the bandwidth utilization alarm value in the outgoing direction set for the interface, the status of the monitoring object is down.

Table 107 Configuring to Monitor Bandwidth Utilization Rate Alarm of Interface

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the Track configuration mode	<b>track track -id</b>	-
Configure bandwidth utilization rate of monitoring interface	<b>interface interface-name</b> <b>trap-threshold [ input   output ]</b>	Mandatory

## Note

- For configurations related to bandwidth alarm value of interface, refer to the interface-related chapter in the User Manual.

### Configure Reachability of Monitoring Route

The monitoring object to be configured in the Track group is route reachability. When there is a route leading to the network configured, the status of the monitoring object is up; otherwise, the status of the monitoring object is down.

Table 4 Configuring to Monitor IPv4 Route Reachability

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the Track configuration mode	<b>track track -id</b>	-
Configure Reachability of Monitoring Route	<b>ip-route ip-address network mask [ vrf vrf-name ] [ metric metric-value ]</b>	Mandatory  If there are metric options, the status of the monitoring object is up only when the metric value of route leading to the network is less than the value configured.

Table 5 Configuring to Monitor IPv6 Route Reachability

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the Track configuration mode	<b>track track -id</b>	-
Configure Reachability of Monitoring Route	<b>ipv6-route ipv6-address/mask-length [ vrf vrf-name ] [ metric metric-value ]</b>	Mandatory  If there are metric options, the status of the monitoring object is up only when the metric value of route leading to the network is less than the value configured.

### Configure Status of Monitoring Aggregation Group

The monitoring object to be configured in the Track group is status of aggregation group. When the status of aggregation group is up, the status of the monitoring object is up; when status of aggregation group is down, the status of the monitoring object is down.

Table 6 Configuring to Monitor Status of Aggregation Group

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the Track configuration mode	<b>track group-id</b>	Mandatory
Configure Status of Monitoring Aggregation Group	<b>link-aggregation link-aggregation-id</b>	Mandatory

### Configure to Monitor Status of Layer-2 Ethernet Interface

The monitoring object to be configured in the Track group is status of layer-2 Ethernet interface. When the layer-2 Ethernet interface is up, the status of the monitoring object is up; when the layer-2 Ethernet interface is down, the status of the monitoring object is down.

Table 7 Configuring to Monitor Status of Layer-2 Ethernet Interface

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the Track configuration mode	<b>track group-id</b>	Mandatory
Configure to Monitor Status of Layer-2 Ethernet Interface	<b>switchport interface-name</b>	Mandatory

### Configure Monitoring RTR Group

The monitoring object to be configured in the Track group is RTR group. When the status of RTR group is up, the status of the monitoring object is up; when status of RTR group is down, the status of the monitoring object is down. RTR (Response Time Reporter) is a network detection and monitoring tool. Track can indirectly monitor network communications by monitoring RTR group.

Table 8 Configuring to Monitor RTR Group

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the Track configuration mode	<b>track track -id</b>	-
Configure Monitoring RTR Group	<b>rtr rtr-group-id</b>	Mandatory

---

### Note

- For configurations related to RTR group, refer to the SLA-related chapter in the User Manual.
- 

### Configure Monitoring BFD Session

The monitoring object to be configured in the Track group is BFD session. When the status of BFD session is up, the status of the monitoring object is up; when status of BFD session is down, the status of the monitoring object is down. BFD protocol is a unified standardized network-wide detection mechanism used to quickly detect and monitor the connections of paths or IP route forwarding in the network. Track can indirectly monitor network connections by monitoring BFD session.

Table 9 Configuring to Monitor Single-hop Session of BFD IPv4

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the Track configuration mode	<b>track track -id</b>	-
Configure Monitoring BFD Session	<b>bfd interface interface-name remote-ip ip-address local-ip ip-address</b>	Mandatory When configuring to monitor BFD session, you are required to configure on both ends of the BFD session; otherwise, the BFD session cannot be successfully established.

Table 10 Configuring to Monitor Single-hop Session of BFD IPv6

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the Track configuration mode	<b>track track -id</b>	-
Configure Monitoring BFD Session	<b>bfd interface interface-name remote-ipv6 ipv6-address local-ipv6 ipv6-address</b>	Mandatory When configuring to monitor BFD session, you are required to configure on both ends of the BFD session; otherwise, the BFD session cannot be successfully established.

Table 11 Configuring to Monitor Multi-hop Session of BFD IPv4

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Enter the Track configuration mode	<b>track track -id</b>	-
Configure Monitoring BFD Session	<b>bfd multihop control</b> <b>remote-ip ip-address local-ip ip-address [multiplier multiplier-value min-transmit-interval minimum-transmit-interval-value min-receive-interval minimum-receive-interval-value]</b>  <b>bfd multihop echo</b> <b>interface interface-name</b> <b>remote-ip ip-address [multiplier multiplier-value min-transmit-interval minimum-transmit-interval-value min-receive-interval minimum-receive-interval-value]</b>	Mandatory  When configuring to monitor BFD session, you are required to configure on both ends of the BFD session; otherwise, the BFD session cannot be successfully established.

### 107.2.3 Track Monitoring and Maintaining

Table 12 Track Monitoring and Maintaining

Command	Description
<b>show track object group-id</b>	Show the information of Track group
<b>show track bfd-session</b>	Show the information of BFD session monitored by Track
<b>show track route-request</b>	Show the information of route monitored by Track

# 108 BFD

---

## 108.1 Overview

BFD (Bidirectional Forwarding Detection) protocol is a unified standardized network-wide detection mechanism used to quickly detect and monitor the connections of paths or IP route forwarding in the network. It provides a universal, standardized, medium-independent, and protocol-independent fast failure detection mechanism, which can quickly detect the line failures between two devices for upper-layer applications (e.g. routing protocols).

BFD can detect failures on any type of paths between systems, and BFD sessions are established based on the needs of upper-layer applications. If multiple application protocols correspond to the same path, a BFD session can be used for detection.

The processing flow of BFD protocol and upper-layer application protocol includes:

- (1) Upper-layer application protocol sends neighbor information (including peer IP address, local IP address, and interface) to the BFD protocol.
- (2) The BFD protocol inquires whether there is a corresponding session. If not, it creates corresponding session based on the neighbor information received. Then the BFD session sends BFD control packets to drive the operation of BFD state machine. The BFD control packets complete corresponding session with a three-way handshake after the transition from Down (start) to Init (initialization) and then to Up (completed). During the process of establishing session, the session parameters are negotiated, including packet sending interval and detection interval.
- (3) After the session is established, the path conditions are detected by periodically sending detection packets. If the BFD control packet sent by the peer device is not received during the detection interval, the BFD protocol will consider the path faulty and advertise the failure information to the upper-layer application protocol.
- (4) After receiving the failure report, the upper-layer application protocol enables the neighbor and notifies the BFD protocol to delete the session when deleting the neighbor. If no other upper-layer protocol needs to detect this session link,

corresponding session will be deleted.

There are two types of detection path, i.e. single-hop path detection and non-single-hop path detection.

## 108.2 BFD Function Configuration

Table 108 BFD Function Configuration List

Configuration Task	
Configure Basic Functions of BFD	Configure Minimum Sending Interval of Single-hop BFD Control Packets
	Configure Minimum Receiving Interval of Single-hop BFD Control Packets
	Configure Detection Timeout Multiple of Single-hop BFD Session
	Configure Authentication Parameter of Single-hop BFD Session
	Configure Minimum Sending Interval of Non-single-hop BFD Control Packets
	Configure Minimum Receiving Interval of Non-single-hop BFD Control Packets
	Configure Detection Timeout Multiple of Non-single-hop BFD Session
	Configure Authentication Parameter of Non-single-hop BFD Session
	Configure Output Interface as Physical Output Interface of BFD Session of Tunnel Interface

### 108.2.1 Configure Basic Functions of BFD

#### Configuration Condition

Before configuring the basic BFD functions, do the following:

- Interface IP addresses have been configured so that neighbor nodes are reachable at the network layer.
- Configure the upper-layer application coordinated with BFD.

### Configure Minimum Sending Interval of Single-hop BFD Control Packets

Table 108 Configuring Minimum Sending Interval of Single-hop BFD Control Packets

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure Minimum Sending Interval of Single-hop BFD Control Packets	<b>bfd min-transmit-interval</b> <i>value</i>	Optional By default, the minimum sending interval of single-hop BFD control packets is 1000 milliseconds.

---

### Note

- The actual sending interval of local BFD packets = MAX (the minimum sending interval of local BFD control packets, and the minimum receiving interval of peer BFD control packets).
- 

### Configure Minimum Receiving Interval of Single-hop BFD Control Packets

Table 108 Configuring Minimum Receiving Interval of Single-hop BFD Control Packets

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure Minimum Receiving Interval of Single-hop BFD Control Packets	<b>bfd min-receive-interval</b> <i>value</i>	Optional By default, the minimum receiving interval of single-hop BFD control packets is 1000 milliseconds.

### Note

- The actual sending interval of peer BFD control packets = MAX (the minimum sending interval of peer BFD control packets, and the minimum receiving interval of local BFD control packets).

### Configure Detection Timeout Multiple of Single-hop BFD Session

Table 108108 Configuring Detection Timeout Multiple of Single-hop BFD Session

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure Detection Timeout Multiple of Single-hop BFD Session	<b>bfd multiplier</b> <i>value</i>	Optional By default, the detection timeout multiple of single-hop BFD session is 5.

### Note

- In order to ensure the effectiveness of BFD session detection, please be careful when configuring the minimum value of BFD detection timeout multiple.
- The actual local BFD detection time = peer BFD session detection timeout multiple × the actual sending interval of peer BFD packets.

### Configure Authentication Parameter of Single-hop BFD Session

Table 108 Configuring Authentication Parameter of Single-hop BFD Session

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure Authentication Parameter of Single-hop BFD Session	<b>bfd authentication</b> <i>key-id</i> { { <b>m-md5</b>   <b>m-sha1</b>   <b>m-sm3</b>   <b>md5</b>   <b>sha1</b>   <b>sm3</b> } { <b>0</b> <i>plain-key</i>   <b>7</b> <i>cipher-key</i> } }   { <b>simple</b> { <b>0</b> <i>plain-password</i>   <b>7</b> <i>cipher-password</i> } }	Optional By default, authentication parameter of single-hop BFD session is not configured.

### Note

- After the BFD authentication function is enabled on the interface, it is valid for the single-hop session based on this interface only.
- In order to ensure BFD authentication can correctly take effect, the authentication information of the interfaces on both ends of the BFD session must be consistent.

### Configure Minimum Sending Interval of Non-single-hop BFD Control Packets

Table 108 Configure Minimum Sending Interval of Non-single-hop BFD Control Packets

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Configure Minimum Sending Interval of Non-single-hop BFD Control Packets	<b>bfd non-single-hop min-transmit-interval</b> <i>value</i>	Optional By default, the minimum sending interval of non-single-hop BFD control packets is 1000 milliseconds.

## Note

- The actual sending interval of local BFD packets = MAX (the minimum sending interval of local BFD control packets, and the minimum receiving interval of peer BFD control packets).
- After configuring the minimum receiving interval of non-single-hop BFD control packets, it will be valid for IPv4/IPv6 multi-hop session and MPLS LSP session. If the minimum receiving interval of non-single-hop BFD control packets is specified in the registered module, it takes effect according to the specified value of the module. If the minimum receiving interval of non-single-hop BFD control packets for the same session is specified in multiple registered modules, it takes effect according to the minimum value specified.

### Configure Minimum Receiving Interval of Non-single-hop BFD Control Packets

Table 108 Configuring Minimum Receiving Interval of Non-single-hop BFD Control Packets

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure Minimum Receiving Interval of Non-single-hop BFD Control Packets	<b>bfd non-single-hop min-receive-interval</b> <i>value</i>	Optional By default, the minimum receiving interval of non-single-hop BFD control packets is 1000 milliseconds.

---

## Note

- The actual sending interval of peer BFD control packets = MAX (the minimum sending interval of peer BFD control packets, and the minimum receiving interval of local BFD control packets).
  - After configuring the minimum sending interval of non-single-hop BFD control packets, it will be valid for IPv4/IPv6 multi-hop session and MPLS LSP session. If the minimum sending interval of non-single-hop BFD control packets is specified in the registered module, it takes effect according to the specified value of the registered module. If the minimum sending interval of non-single-hop BFD control packets for the same session is specified in multiple registered modules, it takes effect according to the minimum value specified.
- 

### Configure Detection Timeout Multiple of Non-single-hop BFD Session

Table 108 Configuring Detection Timeout Multiple of Non-single-hop BFD Session

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure Detection Timeout Multiple of Non-single-hop BFD Session	<b>bfd non-single-hop multiplier <i>value</i></b>	Optional By default, the detection timeout multiple of non-single-hop BFD session is 5.

---

## Note

- In order to ensure the effectiveness of BFD session detection, please be careful when configuring the minimum value of BFD detection timeout multiple.
  - The actual local BFD detection time = peer BFD session detection timeout multiple × the actual sending interval of peer BFD packets.
  - After configuring the detection timeout multiple of non-single-hop BFD session, it will be valid for IPv4/IPv6 multi-hop session and MPLS LSP session. If the detection timeout multiple of non-single-hop BFD session is specified in the registered module, it takes effect according to the specified value of the registered module. If the detection timeout multiple of non-single-hop BFD session for the same session is specified in multiple registered modules, it takes effect according to the minimum value specified.
- 

### Configure Authentication Parameter of Non-single-hop BFD Session

Table 108 Configuring Authentication Parameter of Non-single-hop BFD Session

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure Authentication Parameter of Non-single-hop BFD Session	<b>bfd non-single-hop authentication</b> <i>key-id</i> { { <b>m-md5</b>   <b>m-sha1</b>   <b>m-sm3</b>   <b>md5</b>   <b>sha1</b>   <b>sm3</b> } { <b>0 plain-key</b>   <b>7 cipher-key</b> } }   { <b>simple</b> { <b>0 plain-password</b>   <b>7 cipher-password</b> } }	Optional  By default, authentication parameter of non-single-hop BFD session is not configured.

### Note

- After configuring the non-single-hop BFD authentication function, it will be valid for IPv4/IPv6 multi-hop session and MPLS LSP session.
- In order to ensure BFD authentication can correctly take effect, the authentication information of both ends of the non-single-hop BFD session must be consistent.

### Configure Fast Detection Function of BFD Session

Table 1 Configuring Fast Detection Function of BFD Session

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure fast detection function of BFD session	<b>bfd fast-detect</b>	Optional  By default, the fast detection function of BFD session is disabled.

## 108.2.2 BFD Monitoring and Maintaining

Table 108 BFD Monitoring and Maintaining

Command	Description
<b>show bfd capability</b>	Show the information of BFD capability
<b>show bfd discriminator</b>	Show local identification value of BFD
<b>show bfd session</b>	Show the information of BFD IPv4 session
<b>show bfd session ipv6</b>	Show the information of BFD IPV6 session
<b>show bfd session mpls</b>	Show the information of BFD MPLS session
<b>show bfd session summary</b>	Show the summary of BFD session

## 108.3 Typical Configuration Example of BFD

### 108.3.1 Configure Basic Functions of BFD

#### Network Requirements

- As a connecting device, Device 4 transmits the data in a transparent way.
- OSPF protocol is running on Device1, Device2 and Device3, and BFD detection function is configured on Device1 and Device3.
- Modify BFD parameters. When the line between Device4 and Device3 fails, the service data between Device1 and Device3 can be switched in milliseconds.

#### Network Topology

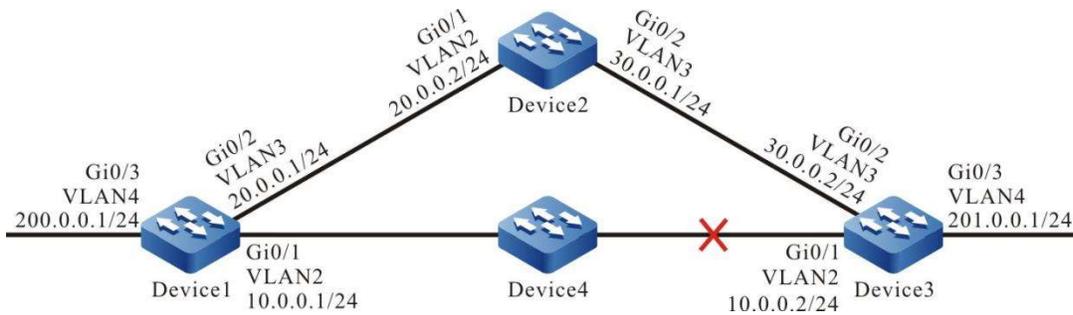


Figure 108 Network Topology for Configuring Basic Functions of BFD

### Configuration Steps

- Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)
- Step 2: Configures IP addresses for the ports. (Omitted)
- Step 3: Configure OSPF.

#### #Configure Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#router-id 1.1.1.1
Device1(config-ospf)#network 10.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 20.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 200.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#exit
```

#### #Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#router-id 2.2.2.2
Device2(config-ospf)#network 20.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#network 30.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#exit
```

#### #Configure Device3.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#router-id 3.3.3.3
Device3(config-ospf)#network 10.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 30.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 201.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#exit
```

- Step 4: Configure coordination of OSPF with BFD.

#### #Configure Device1.

```
Device1(config)#bfd fast-detect
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ip ospf bfd
Device1(config-if-vlan2)#exit
```

### #Configure Device3.

```
Device3(config)#bfd fast-detect
Device3(config)#interface vlan2
Device3(config-if-vlan2)#ip ospf bfd
Device3(config-if-vlan2)#exit
```

### #View the BFD session of Device1.

```
Device1#show bfd session 10.0.0.2 detail
Total session number: 1
OurAddr      NeighAddr      LD/RD      State      Holddown      interface
10.0.0.1     10.0.0.2       12/19      UP         5000          vlan2
Type:direct
Local State:UP Remote State:UP Up for:21h:55m:28s Number of times UP:4
Send Interval:1000ms Detection time:5000ms(1000ms*5)
Local Diag:1 Demand mode:0 Poll bit:0
MinTxInt:1000 MinRxInt:1000 Multiplier:5
Remote MinTxInt:1000 Remote MinRxInt:1000 Remote Multiplier:5
Authentication: Disable
```

Registered modules: OSPF has been successfully coordinated with BFD. The session is established normally, and the detection timeout period is 5 seconds.

### #View the routing table of Device1.

```
Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 10.0.0.0/24 is directly connected, 00:20:01, vlan2
C 20.0.0.0/24 is directly connected, 00:25:22, vlan3
O 30.0.0.0/24 [110/2] via 20.0.0.2, 00:12:31, vlan3
   [110/2] via 10.0.0.2, 00:11:20, vlan2
C 127.0.0.0/8 is directly connected, 00:31:09, lo0
C 200.0.0.0/24 is directly connected, 00:20:10, vlan4
O 201.0.0.0/24 [110/2] via 10.0.0.2, 00:11:30, vlan2
```

According to the routing table, the route 201.0.0.0/24 prefers the lines between Device1 and Device3 for communication.

Step 5: Configure BFD parameters.

#On Device1, change the minimum sending interval and minimum receiving interval of BFD control packets to 100 milliseconds and the detection timeout multiple to 3.

```
Device1(config)#interface vlan2
Device1(config-if-vlan2)#bfd min-transmit-interval 100
Device1(config-if-vlan2)#bfd min-receive-interval 100
Device1(config-if-vlan2)#bfd multiplier 3
Device1(config-if-vlan2)#exit
```

#On Device3, change the minimum sending interval and minimum receiving interval of BFD control packets to 100 milliseconds and the detection timeout multiple to 3.

```
Device3(config)#interface vlan2
Device3(config-if-vlan2)#bfd min-transmit-interval 100
Device3(config-if-vlan2)#bfd min-receive-interval 100
Device3(config-if-vlan2)#bfd multiplier 3
Device3(config-if-vlan2)#exit
```

Step 6: Check the result.

#View the BFD session of Device1.

```
Device1#show bfd session detail
Total session number: 1
OurAddr      NeighAddr      LD/RD      State      Holddown      interface
10.0.0.1      10.0.0.2      12/19      UP          300           vlan2
Type:direct
Local State:UP Remote State:UP Up for: 0h:11m:27s Number of times UP:1
Send Interval:100ms Detection time:300ms(100ms*3)
Local Diag:0 Demand mode:0 Poll bit:0
MinTxInt:100 MinRxInt:100 Multiplier:3
Remote MinTxInt:100 Remote MinRxInt:100 Remote Multiplier:3
Registered protocols:OSPF
```

After the BFD parameters are changed the BFD detection timeout period will be negotiated to 300 milliseconds from 5 seconds.

#When the lines between Device1 and Device3 fail, BFD can quickly identify these failures and notify OSPF which will switch route to Device2 for communication and view the routing table on Device1.

```
Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 10.0.0.0/24 is directly connected, 00:25:00, vlan2
C 20.0.0.0/24 is directly connected, 00:30:33, vlan3
O 30.0.0.0/24 [110/2] via 20.0.0.2, 00:17:32, vlan3
C 127.0.0.0/8 is directly connected, 00:36:10, lo0
C 200.0.0.0/24 is directly connected, 00:25:11, vlan4
O 201.0.0.0/24 [110/3] via 20.0.0.2, 00:00:10, vlan3
```

By comparing with the routing table mentioned in step 3, you will find that the route 201.0.0.0/24 has switched to Device2 for communication.

On Device3, the BFD is processed in a manner which is similar to that on Device1.

# 109 EEP

---

## 109.1 Overview

EEP (Embedded Event Platform) is a extensible and customizable event detection and processing mechanism which is directly provided in the device. It provides a method which enables users to monitor specific event, obtain information and set actions when the event occurs.

## 109.2 EEP Function Configuration

Table109 EEP Function Configuration Task List

Configuration Task	
Configure EEP Policy	Configure EEP Policy
Configure EEP Event	Configure EEP to Bind to Empty Event
	Configure EEP to Bind to Timer Event
	Configure EEP to Bind to TRACK Event
Configure EEP Action	Configure EEP Action

### 109.2.1 Configure EEP Policy

#### Configuration Condition

None

#### Configure EEP Policy

The system can be configured with multiple EEP policies that are independent of each other. In an EEP policy, only an EEP event and at most 50 EEP actions can be configured.

The EEP policy has three states, i.e. init, running and suspend:

- When the EEP policy is created for the first time, its status is init.
- In the EEP policy which has been created, configure EEP event and EEP action, and change the EEP policy status to running. In this status, after detecting the EEP event configured, the EEP policy will perform the EEP actions configured in turn.
- The user can suspend all EEP policies configured or a specified EEP policy with the command **event platform suspend {policy policy-name}**. The EEP policy state changes to suspend. In this status, after detecting the EEP event configured, the EEP policy will not perform the EEP actions configured.

Table 109 Configuring EEP Policy

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Create EEP policy	<b>event platform applet</b> <i>policy-name</i>	Mandatory
Suspend EEP policy	<b>event platform suspend</b> <b>{policy policy-name}</b>	Optional

## 109.2.2 Configure EEP Event

### Configuration Condition

Before configuring the EEP event, do the following:

- Configure EEP policy.

### Configure EEP to Bind to Empty Event

Table 109 Configuring EEP to Bind to Empty Event

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Enter the EEP policy configuration mode	<b>event platform applet</b> <i>policy-name</i>	-
Configure EEP to Bind to Empty Event	<b>event none</b>	Mandatory

## Note

- When EEP is bound to an empty event, the EEP policy will have no event to be monitored. Thus, the user can only trigger the EEP policy bound to empty event to perform EEP action with the command **event platform run** *policy-name*.

### Configure EEP to Bind to Timer Event

The timer event bound to EEP has four types:

- Absolute timer: Trigger timer event when the specified time configured by the user is up.
- Calendar timer: Trigger timer event when the periodic time configured by the user is up.
- Countdown timer: Trigger timer event when the countdown time configured by the user is up.
- Watchdog timer: Trigger timer event when the watchdog time configured by the user is up.

Table 109 Configuring EEP to Bind to Timer Event

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the EEP policy configuration mode	<b>event platform applet</b> <i>policy-name</i>	-

Configure EEP to bind to absolute timer event	<b>event timer absolute</b> <i>year month day hour:minute[:second]</i>	Optional
Configure EEP to bind to calendar timer event	<b>event timer calendar</b> { <b>per-day</b> <i>hour:minute[:second]</i>   <b>per-hour</b> <i>minute</i> / <b>per-month</b> <i>day hour:minute[:second]</i> / <b>per-week</b> <i>week hour:minute[:second]</i> }	Optional Value range of <i>minute</i> : 0~59 Value range of <i>day</i> : 1~28 Value range of <i>week</i> : 0~6, 0 means Sunday
Configure EEP to bind to countdown timer event	<b>event timer countdown</b> <i>time-value</i>	Optional Value range of <i>time-value</i> : 1~107374182, in second
Configure EEP to bind to watchdog timer event	<b>event timer watchdog</b> <i>time-value</i>	Optional Value range of <i>time-value</i> : 1~107374182, in second

### Configure EEP to Bind to TRACK Event

Table 109 Configuring EEP to Bind to TRACK Event

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the EEP policy configuration mode	<b>event platform applet</b> <i>policy-name</i>	-
Configure EEP to Bind to TRACK Event	<b>event track</b> <i>track-id</i> { <i>up-to-down</i> / <i>down-to-up</i> }	Optional Value range of <i>track-id</i> : 1~500

### 109.2.3 Configure EEP Action

Table 109 Configuring EEP Actions

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the EEP policy configuration mode	<b>event platform applet</b> <i>policy-name</i>	-
Configure EEP to perform command line actions	<b>action</b> <i>action-number</i> { <b>cli-command</b> <i>cli-command-string</i>   <b>force-switchover</b>   <b>reload</b> [ <b>master</b>   <b>slave</b> ]   <b>syslog</b> [ <b>msg</b> <i>message-text</i>   <b>priority</b> <i>priority-value</i>   <b>msg</b> <i>message-text</i> ]}	Optional Value range of <i>action-number</i> : 1~1000

---

#### Note

- EEP policy performs command line actions by *action-number* (from small to large).
  - The command line *cli-command-string* is performed in the configured mode by default.
- 

### 109.2.4 EEP Monitoring and Maintaining

Table 109 EEP Monitoring and Maintaining

Command	Description
<b>show eep policy registered</b> { <i>detail</i>   <i>INEXIST-EVENT</i>   <i>NONE-EVENT</i>   <i>TIMER-EVENT</i>   <i>TRACK-EVENT</i> }	View the information of all EEP policy states

## 109.3 Typical Configuration Example of EEP

### 109.3.1 Configure EEP policy and PBR Coordination

#### Network Requirements

- The OSPF protocol is run on all devices, and PBR is configured on Device1.
- By configuring PBR, PC can access the server 2.2.2.2 through Device1 and Device2.
- After EEP is associated with PBR, when the interface of Device1 connecting Device2 is down, EEP quickly notifies PBR to delete the next-hop configuration so that the PC can access the server 2.2.2.2 through Device1 and Device3; when the link between Device1 and Device2 returns to normal, EEP notifies PBR to add the next-hop configuration so that PC can access the server 2.2.2.2 through Device1 and Device2.

#### Network Topology

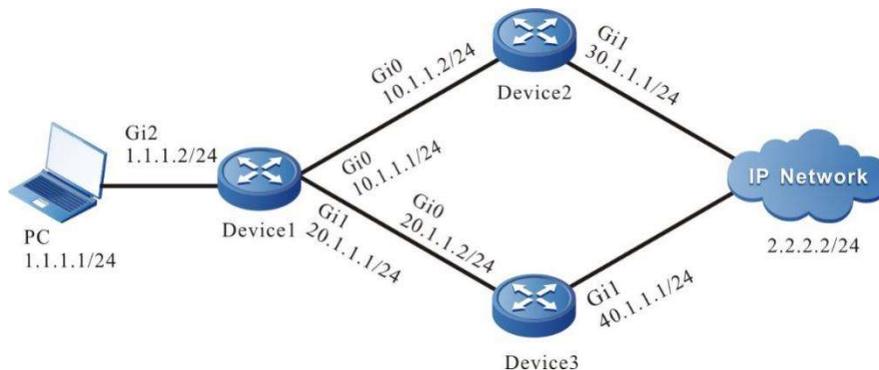


Figure 109 Network Topology for Configuring EEP Policy and PBR Coordination

#### Configuration Steps

Step 1: Configures IP addresses for the ports. (Omitted)

Step 2: Enable the unicast routing protocol OSPF, so that all devices in the network can communicate with each other.

#### #Configure Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#router-id 1.1.1.1
Device1(config-ospf)#network 1.1.1.0 0.0.0.255 area 0
Device1(config-ospf)#network 10.1.1.0 0.0.0.255 area 0
Device1(config-ospf)#network 20.1.1.0 0.0.0.255 area 0
Device1(config-ospf)#exit
```

#### #Configure Device2.

```
Device2#configure terminal
```

```
Device2(config)#router ospf 100
Device1(config-ospf)#router-id 2.2.2.2
Device2(config-ospf)#network 10.1.1.0 0.0.0.255 area 0
Device2(config-ospf)#network 30.1.1.0 0.0.0.255 area 0
Device2(config-ospf)#exit
```

### #Configure Device3.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device1(config-ospf)#router-id 3.3.3.3
Device3(config-ospf)#network 20.1.1.0 0.0.0.255 area 0
Device3(config-ospf)#network 40.1.1.0 0.0.0.255 area 0
Device3(config-ospf)#exit
```

#It can be seen from the routing table of Device1 that there are two next hops that can reach the network 2.2.2.0/24.

```
Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 1.1.1.0/24 is directly connected, 22:14:53, gigabitethernet2
L 1.1.1.1/32 is directly connected, 22:14:53, gigabitethernet2
O 2.2.2.0/24 [110/3] via 10.1.1.2, 00:00:09, gigabitethernet0
   [110/3] via 20.1.1.2, 00:00:09, gigabitethernet1
C 10.1.1.0/24 is directly connected, 21:41:21, gigabitethernet0
L 10.1.1.1/32 is directly connected, 21:41:21, gigabitethernet0
C 20.1.1.0/24 is directly connected, 15:19:15, gigabitethernet1
L 20.1.1.1/32 is directly connected, 15:19:15, gigabitethernet1
O 30.1.1.0/24 [110/2] via 10.1.1.2, 18:55:36, gigabitethernet0
O 40.1.1.0/24 [110/2] via 20.1.1.2, 00:22:08, gigabitethernet1
C 127.0.0.0/8 is directly connected, 87:42:47, lo0
L 127.0.0.1/32 is directly connected, 87:42:47, lo0
```

#On Device1, change the cost value of interface gigabitethernet0 to 100 so that the route leading to the network 2.2.2.0/24 prefers the interface gigabitethernet1.

```
Device1(config)#interface gigabitethernet0
Device1(config-if-gigabitethernet0)#ip ospf cost 100
Device1(config-if-gigabitethernet0)#exit
```

### #View the routing table of Device1.

```
Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 1.1.1.0/24 is directly connected, 23:27:34, gigabitethernet2
L 1.1.1.1/32 is directly connected, 23:27:34, gigabitethernet2
O 2.2.2.0/24 [110/3] via 20.1.1.2, 01:12:50, gigabitethernet1
C 10.1.1.0/24 is directly connected, 22:54:03, gigabitethernet0
L 10.1.1.1/32 is directly connected, 22:54:03, gigabitethernet0
C 20.1.1.0/24 is directly connected, 16:31:57, gigabitethernet1
L 20.1.1.1/32 is directly connected, 16:31:57, gigabitethernet1
O 30.1.1.0/24 [110/3] via 20.1.1.2, 00:31:42, gigabitethernet0
O 40.1.1.0/24 [110/2] via 20.1.1.2, 01:34:50, gigabitethernet1
C 127.0.0.0/8 is directly connected, 88:55:28, lo0
L 127.0.0.1/32 is directly connected, 88:55:28, lo0
```

#On the PC, view with Traceroute the paths through which the server 2.2.2.2 can be reached.

```
C:\Documents and Settings\Administrator>tracert 2.2.2.2

Tracing route to 2.2.2.2 over a maximum of 30 hops

  0  1 ms   1 ms   1 ms  1.1.1.2
  1  <1 ms  <1 ms  <1 ms  20.1.1.2
  .
  .
  .
  n  <1 ms  <1 ms  <1 ms  2.2.2.2
Trace complete.
```

It is indicated that PC can access the server 2.2.2.2 through Device1 and Device3.

Step 3: Configure policy route on Device1.

#Configure the access control list 1001 and permit PC to access the network 2.2.2.0/24.

```
Device1(config)#ip access-list extended 1001
Device1(config-ext-nacl)#permit ip any 2.2.2.0 0.0.0.255
Device1(config-ext-nacl)#exit
```

#Configure the policy route aaa, associate with the access control list 1001, and specify the next hop as 10.1.1.2.

```
Device1(config)#route-policy aaa permit 10
Device1(config-pbr)#match ip address acl 1001
Device1(config-pbr)#set ip next-hop 10.1.1.2
Device1(config-pbr)#exit
```

#View the information of the policy route aaa of Device1.

```
Device1#show route-policy aaa
route-policy aaa
sequence 10 permit:
  match ip address acl 1001
  set ip next-hop 10.1.1.2
```

Step 4: Apply the policy route.

#Apply the policy route aaa on the interface gigabitethernet2 of Device1.

```
Device1(config)#interface gigabitethernet2
Device1(config-if-gigabitethernet2)#ip policy aaa
Device1(config-if-gigabitethernet2)#exit
```

#On the PC, view with Traceroute the paths through which the server 2.2.2.2 can be reached.

```
C:\Documents and Settings\Administrator>tracert 2.2.2.2

Tracing route to 2.2.2.2 over a maximum of 30 hops

  0  1 ms   1 ms   1 ms  1.1.1.2
  1  <1 ms  <1 ms  <1 ms  10.1.1.2
  .
  .
  .
  n  <1 ms  <1 ms  <1 ms  2.2.2.2
Trace complete.
```

It is indicated that after the policy route is applied on the interface gigabitethernet2, PC can access the server 2.2.2.2 through Device1 and Device2.

Step 5: Configure EEP policy to associate with PBR.

#Configure TRACK 1 to monitor the status of interface gigabitethernet 0.

```
Device1(config)#track 1
Device1(config-track)#interface gigabitethernet0 line-protocol
Device1(config-track)#exit
```

#Configure EEP policy e1 on Device1 to bind to track group 1 to monitor the status of interface gigabitethernet0. When the interface gigabitethernet0 of Device1 is down, notify PBR to delete corresponding next-hop configuration.

```
Device1(config)#event platform applet e1
Device1(config-EEP)#event track 1 up-to-down
Device1(config-EEP)#action 1 cli-command route-policy aaa permit 10
Device1(config-EEP)#action 2 cli-command no set ip next-hop 10.1.1.2
Device1(config-EEP)#exit
```

#Configure EEP policy e2 on Device1 to bind to track group 1 to monitor the status of interface gigabitethernet0. When the interface gigabitethernet0 of Device1 is up, notify PBR to add corresponding next-hop configuration.

```
Device1(config)#event platform applet e2
Device1(config-EEP)#event track 1 down-to-up
Warning:
Configuring event track 1 down-to-up is risky, are you sure to configure?(Yes/No)yes
Device1(config-EEP)#action 1 cli-command route-policy aaa permit 10
Device1(config-EEP)#action 2 cli-command set ip next-hop 10.1.1.2
Device1(config-EEP)#exit
```

Step 6: Check the result.

#When interface gigabitethernet0 of Device1 is down, EEP will quickly notify PBR to delete the next-hop configuration, and PC will access the server 2.2.2.2 through Device3.

```
Device1#show route-policy aaa
route-policy aaa
sequence 10 permit:
match ip address acl 1001
```

#On the PC, view with Traceroute the paths through which the server 2.2.2.2 can be reached.

```
C:\Documents and Settings\Administrator>tracert 2.2.2.2

Tracing route to 2.2.2.2 over a maximum of 30 hops

  0  1 ms   1 ms   1 ms  1.1.1.2
  1  <1 ms  <1 ms  <1 ms  20.1.1.2
  ...
  n  <1 ms  <1 ms  <1 ms  2.2.2.2
Trace complete.
```

It is indicated that after interface gigabitethernet2 becomes down, PC can access the server 2.2.2.2 through Device1 and Device3.

#When interface gigabitethernet0 of Device1 is up, EEP will notify PBR to add the next-hop configuration, and PC will access the server 2.2.2.2 through Device2.

```
Device1#show route-policy aaa
route-policy aaa
sequence 10 permit:
  match ip address acl 1001
  set ip next-hop 10.1.1.2
```

#On the PC, view with Traceroute the paths through which the server 2.2.2.2 can be reached.

```
C:\Documents and Settings\Administrator>tracert 2.2.2.2
```

```
Tracing route to 2.2.2.2 over a maximum of 30 hops
```

```
  0  1 ms  1 ms  1 ms  1.1.1.2
  1  <1 ms  <1 ms  <1 ms  10.1.1.2
  . . . . .
  n  <1 ms  <1 ms  <1 ms  2.2.2.2
Trace complete.
```

It is indicated that after interface gigabitethernet2 becomes up, PC can access the server 2.2.2.2 through Device1 and Device2.

# 110 ERPS

---

## 110.1 Overview

In the Ethernet layer-2 network, STP (Spanning Tree Protocol) is generally used for network reliability. However, the convergence time of STP, in second, is long when there is a large network diameter. In order to reduce the convergence time and eliminate the influence of network size, ERPS (Ethernet Ring Protection Switching) technology is born. ERPS is a layer-2 damage protocol standard defined by ITU-T, with a protocol standard number of ITU-T G.8032/Y1344. It is also called G.8032 which is a reliable and stable Ethernet link layer technology. When the Ethernet ring network is complete, it can prevent the broadcast storm caused by data loop. When the Ethernet ring network link fails, with a high convergence speed, it can quickly restore the communication path between the nodes on the ring network. At the same time, if the manufacturer's devices within the ring network all support this protocol, interconnection can be achieved.

## Definitions of ERPS-related concepts:

- ERPS ring, a basic unit of ERPS protocol, is a group of interconnected network devices configured with the same control VLAN (Virtual Local Area Network). It has main ring and subring. The former is closed, while the latter is not closed. The attributes of main ring and subring are determined by users.
- Port role: According to the ERPS protocol, there are three types of port roles, i.e. RPL owner port, RPL neighbor port, and general port. In particular, RPL neighbor port is supported by ERPSv2 only.
- RPL owner port: An ERPS ring has one RPL owner port only, specified by users. The ERPS protocol prevents link loops by blocking the forwarding state of the RPL owner port. The link where the RPL owner port is located is the RPL (Ring Protection Link).
- RPL neighbor port means the node port directly connected to the RPL owner port. Normally, both RPL owner port and RPL neighbor port will be blocked to prevent loops. When the ERPS ring network fails, both RPL owner port and RPL neighbor port will be unblocked.
- General port: In the ERPS ring, all ports except RPL owner and RPL neighbor are general ports. They are responsible for monitoring the status of their own direct links and notify other node ports of the changes in a timely manner.
- ERPS control VLAN is used to transmit ERPS protocol packets. Control VLAN is specified by users. ERPS control VLAN (Virtual Local Area Network) cannot be used for other services. Each ERPS ring has a different control VLAN.
- ERPS data instance is a data instance mapped by data VLAN which requires ERPS ring protection.

## 110.2 ERPS Function Configuration

Table 110 ERPS Function Configuration List

Configuration Task	
Configure ERPS Ring	Configure ERPS Ring
	Enable ERPS Protocol
Configure ERPS Ring Timer	Configure ERPS Ring Timer
Configure ERPS Network Optimization	Configure ERPS Port Block Switch Mode

	Clear Blocking Point Configured for ERPS
	Configure ERPS Topology Change Advertisement
	Configure ERPS TC Limiting Function
Configure Coordination of ERPS with CFM	Configure ERPS to Coordinate with CFM

### 110.2.1 Configure ERPS Ring

When configuring ERPS ring, you are required to configure the ports accessing ERPS ring on each node and the nodes on the ring.

#### Configuration Condition

Before configuring ERPS ring, do the following:

- Create control VLAN;
- Close the ring network protocol of ring port;
- Configure the ring port as trunk mode;
- Add the ring port to the control VLAN to which the ring belongs;
- Configure the mapping relationship between MSTP instance and the VLAN to be included.

#### Configure ERPS Ring

Configure basic functions of ERPS ring

Table 110 Configuring ERPS Ring

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Create ERPS ring	<b>erps ring <i>ring-id</i></b>	Mandatory By default, no ERPS ring is created, and

		the value range of the ring is 1~64.
Configure the control VLAN of ERPS ring	<b>control vlan</b> <i>vlan-id</i>	Mandatory  By default, no control VLAN of ERPS ring is configured.
Configure the data instance of ERPS ring	<b>instance</b> <i>instance-list</i>	Mandatory  By default, no data instance of ERPS ring is configured.
Configure port PORT0 of ERPS ring	<b>port0</b> { <b>interface</b> <i>interface-name</i>   interface <b>link-aggregation</b> <i>link-aggregation-id</i> } [ <b>rpl</b> { <b>owner</b>   <b>neighbour</b> } ]	Mandatory  By default, no port PORT0 of ERPS ring is configured.  <b>rpl owner:</b> owner port, the port of which is RPL  <b>rpl neighbour:</b> neighbour port, the port of which is RPL  It is a general port if no rpl is configured.
Configure port PORT1 of ERPS ring	<b>port1</b> { <b>interface</b> <i>interface-name</i>   interface <b>link-aggregation</b> <i>link-aggregation-id</i> } [ <b>rpl</b> { <b>owner</b>   <b>neighbour</b> } ]	Mandatory  By default, ERPS port1 is not configured.  <b>rpl owner:</b> owner port, the port of which is RPL  <b>rpl neighbour:</b> neighbour port, the port of which is RPL

		It is a general port if no rpl is configured.
Configure ERPS ring version	<b>version { v1 / v2 }</b>	Optional By default, the version is version v2.
Configure the mel value of ERPS ring packet	<b>mel level-id</b>	Optional By default, the mel value is 7, and the value range is 0~7.
Configure the ERPS ring as a subring	<b>sub-ring</b>	Optional By default, the ERPS ring is a main ring.
Configure the non-revertive mode of ERPS ring	<b>revertive disable</b>	Optional By default, ERPS is in revertive mode.
Configure the virtual channel of ERPS subring	<b>virtual-channel enable</b>	Optional By default, ERPS has a non-virtual channel.

---

## Note

- ERPS control VLAN is used to transmit ERPS protocol packets only rather than for other services. All the nodes in the same ERPS ring need to be configured with the same mel value.
  - In the networking environment with intersecting rings, virtual channel of subring is not recommended for networking.
- 

### Enable ERPS Protocol

Upon completion of the configuration mentioned above, use this command to enable ERPS protocol.

Table 110 Enabling Protocol on ERPS Ring

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the ERPS configuration mode	<b>erps ring <i>ring-id</i></b>	-
Enable ERPS Protocol	<b>erps enable</b>	Mandatory By default, the ERPS protocol is not enabled on the ring.

## 110.2.2 Configure ERPS Ring Timer

### Configuration Condition

Before configuring ERPS timer, do the following:

- Configure ERPS ring.

### Configure ERPS Ring Timer

After the node device or link failure in the ERPS ring is recovered, in order to prevent network flapping, the ERPS ring timer will be enabled to reduce the interruption time of service traffic.

Table 110 Configuring ERPS Ring Timer

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the ERPS configuration mode	<b>erps ring <i>ring-id</i></b>	-
Configure Guard timer of ERPS ring	<b>guard-timer <i>time-value</i></b>	Mandatory By default, the timeout period of the Guard timer is 500 milliseconds, and the range of the Guard

		timer is 10 to 2000 milliseconds.
Configure Hold-off timer of ERPS ring	<b>holdoff-timer</b> <i>time-value</i>	Mandatory  By default, the timeout period of the Hold-off timer is 0 millisecond, and the range of the Guard timer is 0 ~ 10000 milliseconds.
Configure WTR timer of ERPS ring	<b>wtr-timer</b> <i>time-value</i>	Mandatory  By default, the timeout period of the Guard timer is 5 minutes, and the range of the WTR timer is 1 ~ 12 minutes.

### 110.2.3 Configure ERPS Network Optimization

#### Configuration Condition

Before configuring ERPS network optimization, ensure that:

- Configure ERPS ring.

#### Configure ERPS Port Block Switch Mode

Since the bandwidth of the link where the RPL owner port is located may carry more user traffic, you may consider blocking the link with a low bandwidth so that the user traffic can go back to RPL for transmission.

Table 110 Configuring ERPS Port Block Switch Mode

Step	Command	Description
Configure ERPS Port Block Switch Mode	<b>erps ring</b> <i>ring-id</i> { <b>interface</b> <i>interface-name</i>   <b>interface link-aggregation</b> <i>link-</i>	Mandatory  By default, the ERPS port blocking point

	<i>aggregation-id</i> } <b>switch</b> { <b>force</b>   <b>manual</b> }	switch mode is not configured.
--	---	--------------------------------

### Clear Blocking Point Configured for ERPS

Clear the blocking point switch operation configured for ERPS ring.

Table 110 Clearing Blocking Point Configured for ERPS

Step	Command	Description
Clear Blocking Point Configured for ERPS	<b>clear erps ring</b> <i>ring-id</i>	Mandatory

### Configure ERPS Topology Change Advertisement

When the topology of the ERPS ring changes without notifying layer-2 network in time, the MAC address entries before the downstream network topology changes still remain in the MAC address table of layer-2 network, which will cause interruption of user traffic. In order to ensure the normal communication of user traffic, you are required to select the topology change notification object of the ERPS ring according to the user's actual network.

Table 110 Configuring ERPS Ring Topology Change Advertisement

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the ERPS configuration mode	<b>erps ring</b> <i>ring-id</i>	-
Configure ERPS ring topology change advertisement	<b>tc-notify erps ring</b> <i>ring-list</i>	Mandatory By default, the ERPS topology change is not notified.

### Configure ERPS TC Limiting Function

Frequent topology change notifications will result in a decrease in CPU processing capacity and the frequent refreshing of Flush-FDB packets on the ERPS ring to occupy network bandwidth. To avoid this situation, topology change notification packets should be suppressed. The device is protected by configuring the ERPS topology change protection interval and the maximum threshold value for processing topology change packets within the topology change protection interval, and avoiding frequent deletion of MAC address entries and ARP entries.

Table 110 Configuring ERPS TC Limiting Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the ERPS configuration mode	<b>erps ring</b> <i>ring-id</i>	-
Configure to enable the ERPS topology change TC limiting function	<b>tc-limit enable</b>	Mandatory  By default, the TC limiting function is not enabled.
Configure the timer interval of ERPS topology change TC limit	<b>tc-limit interval</b> <i>interval-value</i>	Optional  By default, the time interval is 2 seconds, and the value range is 1~500 seconds.
Configure the threshold value of ERPS topology change TC limit	<b>tc-limit threshold</b> <i>threshold-value</i>	Optional  The default value is 3, and the value range is 1~64.

## 110.2.4 Configure Coordination of ERPS with CFM

### Configuration Condition

Before configuring the coordination of ERPS with CFM (Connectivity Fault Management), do the following:

- Configure basic ERPS functions.
- Configure CFM function

### Configure Coordination of ERPS with CFM

After configuring the Ethernet CFM coordination function on the ring port added to ERPS ring, you can accelerate the detection of failures to realize the fast convergence of topology and reduce the interruption time of traffic.

Table 110 Configuring Coordination of ERPS with CFM

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Configure Coordination of ERPS with CFM	<b>erps ring</b> <i>ring-id</i> <b>track cfm domain</b> <i>domain-name</i> <b>service-instance</b> <i>ser-name</i> <b>mep</b> <i>mep-id</i> <b>remote-mep</b> <i>rmep-id</i>	Mandatory  By default, the port is not coordinated with CFM.

## 110.2.5 ERPS Monitoring and Maintaining

Table 110 ERPS Monitoring and Maintaining

Command	Description
<b>clear erps [ring ring-id ] statistics</b>	Clear ERPS-related statistics
<b>show erps [ ring ring-id ] config</b>	Show the ERPS configuration information
<b>show erps [ring ring-id] detail</b>	Show the detailed information of ERPS
<b>show erps [ring ring-id] statistics</b>	Show the ERPS statistics

## 110.3 Typical Configuration Example of ERPS

### 110.3.1 Configure Basic Functions of ERPS

#### Network Requirements

- All Devices are within the same layer-2 network.
- ERPS is enabled on all Devices and used to disconnect the link loop in the network.

#### Network Topology

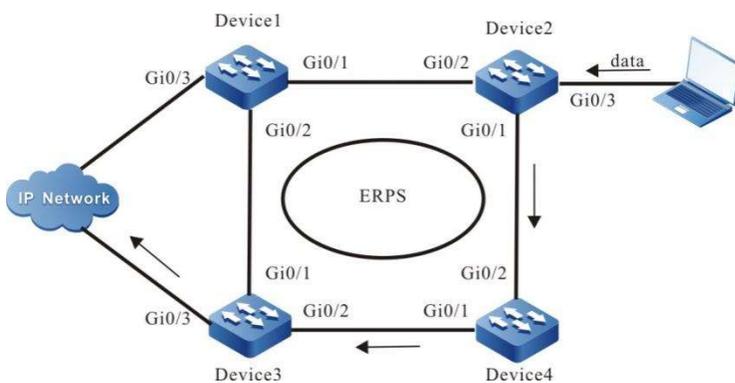


Figure 110 Configuring Basic Functions of ERPS

#### Configuration Steps

Step 1: Configure VLANs, and configure the link type of the ports.

#On Device1, create VLAN2 and VLAN100~VLAN200, configure the link type of ports gigabitethernet0/1 and gigabitethernet0/2 as Trunk, permitting services of VLAN2 and VLAN100~VLAN200 to pass, and disable the spanning tree and storm suppression under the port.

```
Device1#configure terminal
Device1(config)#vlan 2,100-200
Device1(config)# interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#shutdown
Device1(config-if-gigabitethernet0/1)# switchport mode trunk
Device1(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device1(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device1(config-if-gigabitethernet0/1)# no storm-control unicast
Device1(config-if-gigabitethernet0/1)# no storm-control broadcast
Device1(config-if-gigabitethernet0/1)# no storm-control multicast
Device1(config-if-gigabitethernet0/1)# no spanning-tree enable
Device1(config-if-gigabitethernet0/1)#exit
Device1(config)# interface gigabitethernet 0/2
Device1(config-if-gigabitethernet0/2)# switchport mode trunk
Device1(config-if-gigabitethernet0/2)# no switchport trunk allowed vlan all
Device1(config-if-gigabitethernet0/2)# switchport trunk allowed vlan add 2,100-200
Device1(config-if-gigabitethernet0/2)# no storm-control unicast
Device1(config-if-gigabitethernet0/1)# no storm-control broadcast
Device1(config-if-gigabitethernet0/1)# no storm-control multicast
Device1(config-if-gigabitethernet0/2)# no spanning-tree enable
Device1(config-if-gigabitethernet0/2)#end
```

#On Device2, create VLAN2 and VLAN100~VLAN200, configure the link type of ports gigabitethernet0/1 and gigabitethernet0/2 as Trunk, permitting services of VLAN2 and VLAN100~VLAN200 to pass, and disable the spanning tree and storm suppression under the port.

```
Device2#configure terminal
Device2 (config)#vlan 2,100-200
Device2 (config)# interface gigabitethernet 0/1
Device2 (config-if-gigabitethernet0/1)#shutdown
Device2 (config-if-gigabitethernet0/1)# switchport mode trunk
Device2 (config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device2 (config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device2 (config-if-gigabitethernet0/1)# no storm-control unicast
Device2(config-if-gigabitethernet0/1)# no storm-control broadcast
Device2(config-if-gigabitethernet0/1)# no storm-control multicast
Device2 (config-if-gigabitethernet0/1)# no spanning-tree enable
Device2 (config-if-gigabitethernet0/1)#exit
Device2 (config)# interface gigabitethernet 0/2
Device2 (config-if-gigabitethernet0/2)# switchport mode trunk
Device2 (config-if-gigabitethernet0/2)# no switchport trunk allowed vlan all
Device2 (config-if-gigabitethernet0/2)# switchport trunk allowed vlan add 2,100-200
Device2 (config-if-gigabitethernet0/2)# no storm-control unicast
Device2(config-if-gigabitethernet0/1)# no storm-control broadcast
Device2(config-if-gigabitethernet0/1)# no storm-control multicast
Device2 (config-if-gigabitethernet0/2)# no spanning-tree enable
Device2 (config-if-gigabitethernet0/2)#end
```

#On Device3, create VLAN2 and VLAN100~VLAN200, configure the link type of ports gigabitethernet0/1 and gigabitethernet0/2 as Trunk, permitting services of VLAN2 and VLAN100~VLAN200 to pass, and disable the spanning tree and storm suppression under the port.

```
Device3#configure terminal
Device3 (config)#vlan 2,100-200
Device3 (config)# interface gigabitethernet 0/1
Device3 (config-if-gigabitethernet0/1)#shutdown
```

```

Device3 (config-if-gigabitethernet0/1)# switchport mode trunk
Device3 (config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device3 (config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device3 (config-if-gigabitethernet0/1)# no storm-control unicast
Device3 (config-if-gigabitethernet0/1)# no storm-control broadcast
Device3 (config-if-gigabitethernet0/1)# no storm-control multicast
Device3 (config-if-gigabitethernet0/1)# no spanning-tree enable
Device3 (config-if-gigabitethernet0/1)# exit
Device3 (config)# interface gigabitethernet 0/2
Device3 (config-if-gigabitethernet0/2)# switchport mode trunk
Device3 (config-if-gigabitethernet0/2)# no switchport trunk allowed vlan all
Device3 (config-if-gigabitethernet0/2)# switchport trunk allowed vlan add 2,100-200
Device3 (config-if-gigabitethernet0/2)# no storm-control unicast
Device3 (config-if-gigabitethernet0/2)# no storm-control broadcast
Device3 (config-if-gigabitethernet0/2)# no storm-control multicast
Device3 (config-if-gigabitethernet0/2)# no spanning-tree enable
Device3 (config-if-gigabitethernet0/2)# end

```

#On Device4, create VLAN2 and VLAN100~VLAN200, configure the link type of ports gigabitethernet0/1 and gigabitethernet0/2 as Trunk, permitting services of VLAN2 and VLAN100~VLAN200 to pass, and disable the spanning tree and storm suppression under the port.

```

Device4#configure terminal
Device4 (config)#vlan 2,100-200
Device4 (config)# interface gigabitethernet 0/1
Device4 (config-if-gigabitethernet0/1)#shutdown
Device4 (config-if-gigabitethernet0/1)# switchport mode trunk
Device4 (config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device4 (config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device4 (config-if-gigabitethernet0/1)# no storm-control unicast
Device4 (config-if-gigabitethernet0/1)# no storm-control broadcast
Device4 (config-if-gigabitethernet0/1)# no storm-control multicast
Device4 (config-if-gigabitethernet0/1)# no spanning-tree enable
Device4 (config-if-gigabitethernet0/1)# exit
Device4 (config)# interface gigabitethernet 0/2
Device4 (config-if-gigabitethernet0/2)# switchport mode trunk
Device4 (config-if-gigabitethernet0/2)# no switchport trunk allowed vlan all
Device4 (config-if-gigabitethernet0/2)# switchport trunk allowed vlan add 2,100-200
Device4 (config-if-gigabitethernet0/2)# no storm-control unicast
Device4 (config-if-gigabitethernet0/2)# no storm-control broadcast
Device4 (config-if-gigabitethernet0/2)# no storm-control multicast
Device4 (config-if-gigabitethernet0/2)# no spanning-tree enable
Device4 (config-if-gigabitethernet0/2)# end

```

Step 2: Configure MST instance.

#On Device1, configure MST instance 1 to map vlan100-200, and activate the instance.

```

Device1#configure terminal
Device1 (config)# spanning-tree mst configuration
Device1 (config-mst)# instance 1 vlan 100-200
Device1 (config-mst)# active configuration pending
Device1 (config-mst)# end

```

#On Device2, configure MST instance 1 to map vlan100-200, and activate the instance.

```

Device2#configure terminal
Device2 (config)# spanning-tree mst configuration
Device2 (config-mst)# instance 1 vlan 100-200
Device2 (config-mst)# active configuration pending

```

```
Device2 (config-mst)#end
```

#On Device3, configure MST instance 1 to map vlan100-200, and activate the instance.

```
Device3#configure terminal
Device3 (config)# spanning-tree mst configuration
Device3 (config-mst)# instance 1 vlan 100-200
Device3 (config-mst)# active configuration pending
Device3 (config-mst)#end
```

#On Device4, configure MST instance 1 to map vlan100-200, and activate the instance.

```
Device4#configure terminal
Device4 (config)# spanning-tree mst configuration
Device4 (config-mst)# instance 1 vlan 100-200
Device4 (config-mst)# active configuration pending
Device4 (config-mst)#end
```

### Step 3: Configure ERPS.

#On Device1, configure ERPS ring1. Configure vlan2 as the control vlan of ring1, gigabitethernet0/1 as the normal port of ring1, gigabitethernet0/2 as the owner port of ring1, and instance 1 as the data vlan of ring1; enable the ERPS function of ring1.

```
Device1# configure terminal
Device1(config)#erps ring 1
Device1(config-erps1)# control vlan 2
Device1(config-erps1)# port0 interface g0/1
Device1(config-erps1)# port1 interface g0/2 rpl owner
Device1(config-erps1)# instance 1
Device1(config-erps1)# erps enable
Device1(config-erps1)# exit
Device1(config)# interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#no shutdown
Device1(config-if-gigabitethernet0/1)# end
```

#On Device2, configure ERPS ring1. Configure vlan2 as the control vlan of ring1, gigabitethernet0/1 as the normal port of ring1, gigabitethernet0/2 as the normal port of ring1, and instance 1 as the data vlan of ring1; enable the ERPS function of ring1.

```
Device2# configure terminal
Device2(config)#erps ring 1
Device2(config-erps1)# control vlan 2
Device2(config-erps1)# port0 interface g0/2
Device2(config-erps1)# port1 interface g0/1
Device2(config-erps1)# instance 1
Device2(config-erps1)# erps enable
Device2(config-erps1)# exit
Device2(config)# interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#no shutdown
Device2(config-if-gigabitethernet0/1)# end
```

#On Device3, configure ERPS ring1. Configure vlan2 as the control vlan of ring1, gigabitethernet0/1 as the neighbor port of ring1, gigabitethernet0/2 as the normal port of ring1, and instance 1 as the data vlan of ring1; enable the ERPS function of ring1.

```
Device3# configure terminal
Device3(config)#erps ring 1
Device3(config-erps1)# control vlan 2
Device3(config-erps1)# port0 interface g0/1 rpl neighbor
```

```

Device3(config-erps1)# port1 interface g0/2
Device3(config-erps1)# instance 1
Device3(config-erps1)# erps enable
Device3(config-erps1)# exit
Device3(config)# interface gigabitethernet 0/1
Device3(config-if-gigabitethernet0/1)#no shutdown
Device3(config-if-gigabitethernet0/1)# end

```

#On Device4, configure ERPS ring1. Configure vlan2 as the control vlan of ring1, gigabitethernet0/1 as the normal port of ring1, gigabitethernet0/2 as the normal port of ring1, and instance 1 as the data vlan of ring1; enable the ERPS function of ring1.

```

Device4# configure terminal
Device4(config)#erps ring 1
Device4(config-erps1)# control vlan 2
Device4(config-erps1)# port0 interface g0/1
Device4(config-erps1)# port1 interface g0/2
Device4(config-erps1)# instance 1
Device4(config-erps1)# erps enable
Device4(config-erps1)# exit
Device4(config)# interface gigabitethernet 0/1
Device4(config-if-gigabitethernet0/1)#no shutdown
Device4(config-if-gigabitethernet0/1)# end

```

Step 4: Check the result.

#After the network topology is stable, check the ERPS information of the Device. Take Device1 as an example.

#View the ERPS information of Device1.

```

Device1# show erps ring 1 detail
Ring ID      : 1
Version      : v2
R-APS mel    : 7
Instance     : 1 vlans mapped : 100-200
Control VLAN : 2
Node role    : Owner
Node state   : idle
Guard timer  : 500 ms      Running : 0 ms
Holdoff timer : 0 ms      Running : 0 ms
WTR timer    : 5 min      Running : 0 s
WTB timer    : 7 s        Running : 0 s
Subring      : No
Tc-limit enable : No
Tc-limit Interval : 2
Tc-limit Threshold : 3
Revertive operation : Revertive
R-APS channel : Non-Virtual channel
Enable status : Enable
Gigabitethernet0/1 Flush Logic
  Remote Node ID : 0000-0000-0000
  Remote BPR     : 0
Gigabitethernet0/1 track CFM
  MD Name       :
  MA Name       :
  MEP ID        : 0
  RMEP ID       : 0
  CFM State     : 0

```

```
GigabitEthernet0/2 Flush Logic
  Remote Node ID : 0000-0000-0000
  Remote BPR   : 0
GigabitEthernet0/2 track CFM
  MD Name :
  MA Name :
  MEP ID  : 0
  RMEP ID : 0
  CFM State : 0
```

Port	Name	PortRole	SwitchType	PortStatus	SignalStatus
Port0	gigabitEthernet0/1	Normal	--	Forwarding	Non-failed
Port1	gigabitEthernet0/2	Owner	--	Blocking	Non-failed

## Note

- Before configuring ERPS, ensure the link status of at least one point in the ring network is down. Otherwise, there will be loops.

### 110.3.2 Configure ERPS Load

#### Network Requirements

- All devices are within the same layer-2 network.
- The data traffic of Data1 is transmitted through Device2-Device1, and that of Data2 is transmitted through Device4-Device3 to achieve load sharing and provide link backup.

#### Network Topology

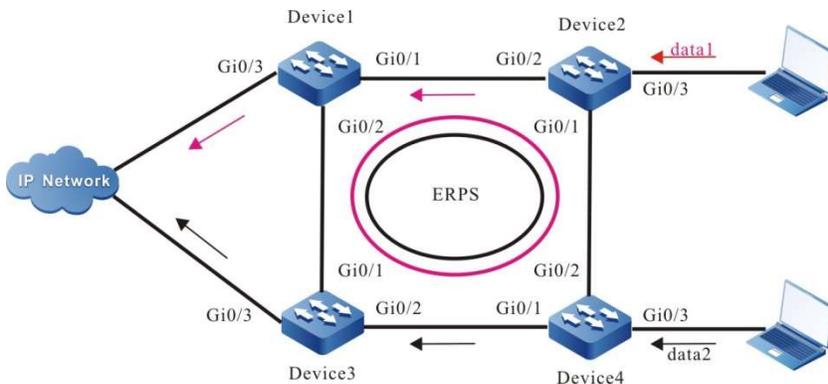


Figure 110 Configuring ERPS Load

#### Configuration Steps

Step 1: Configure VLANs, and configure the link type of the ports.

#On Device1, create VLAN2~VLAN3, VLAN100~VLAN200 and VLAN300~VLAN400, configure the link type of ports gigabitethernet0/1 and gigabitethernet0/2 as Trunk, permitting services of VLAN2~VLAN3, VLAN100~VLAN200 and VLAN300~VLAN400 to pass, and disable the spanning tree and storm suppression under the port.

```
Device1#configure terminal
Device1(config)#vlan 2-3,100-200,300-400
Device1(config)# interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#shutdown
Device1(config-if-gigabitethernet0/1)# switchport mode trunk
Device1(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device1(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device1(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 3,300-400
Device1(config-if-gigabitethernet0/1)# no storm-control unicast
Device1(config-if-gigabitethernet0/1)# no storm-control broadcast
Device1(config-if-gigabitethernet0/1)# no storm-control multicast
Device1(config-if-gigabitethernet0/1)# no spanning-tree enable
Device1(config-if-gigabitethernet0/1)#exit
Device1(config)# interface gigabitethernet 0/2
Device1(config-if-gigabitethernet0/1)# switchport mode trunk
Device1(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device1(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device1(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 3,300-400
Device1(config-if-gigabitethernet0/1)# no storm-control unicast
Device1(config-if-gigabitethernet0/1)# no storm-control broadcast
Device1(config-if-gigabitethernet0/1)# no storm-control multicast
Device1(config-if-gigabitethernet0/1)# no spanning-tree enable
Device1(config-if-gigabitethernet0/1)#end
```

#On Device2, create VLAN2~VLAN3, VLAN100~VLAN200 and VLAN300~VLAN400, configure the link type of ports gigabitethernet0/1 and gigabitethernet0/2 as Trunk, permitting services of VLAN2~VLAN3, VLAN100~VLAN200 and VLAN300~VLAN400 to pass, and disable the spanning tree and storm suppression under the port.

```
Device2#configure terminal
Device2(config)# vlan 2-3,100-200,300-400
Device2(config)# interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#shutdown
Device2(config-if-gigabitethernet0/1)# switchport mode trunk
Device2(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device2(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device2(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 3,300-400
Device2(config-if-gigabitethernet0/1)# no storm-control unicast
Device2(config-if-gigabitethernet0/1)# no storm-control broadcast
Device2(config-if-gigabitethernet0/1)# no storm-control multicast
Device2(config-if-gigabitethernet0/1)# no spanning-tree enable
Device2(config-if-gigabitethernet0/1)#exit
Device2(config)# interface gigabitethernet 0/2
Device2(config-if-gigabitethernet0/1)# switchport mode trunk
Device2(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device2(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device2(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 3,300-400
Device2(config-if-gigabitethernet0/1)# no storm-control unicast
Device2(config-if-gigabitethernet0/1)# no storm-control broadcast
Device2(config-if-gigabitethernet0/1)# no storm-control multicast
Device2(config-if-gigabitethernet0/1)# no spanning-tree enable
Device2(config-if-gigabitethernet0/1)#end
```

#On Device3, create VLAN2~VLAN3, VLAN100~VLAN200 and VLAN300~VLAN400, configure the link type of ports gigabitethernet0/1 and gigabitethernet0/2 as Trunk, permitting services of VLAN2~VLAN3,

VLAN100~VLAN200 and VLAN300~VLAN400 to pass, and disable the spanning tree and storm suppression under the port.

```
Device3#configure terminal
Device3(config)# vlan 2-3,100-200,300-400
Device3(config)# interface gigabitethernet 0/1
Device3(config-if-gigabitethernet0/1)#shutdown
Device3(config-if-gigabitethernet0/1)# switchport mode trunk
Device3(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device3(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device3(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 3,300-400
Device3(config-if-gigabitethernet0/1)# no storm-control unicast
Device3(config-if-gigabitethernet0/1)# no storm-control broadcast
Device3(config-if-gigabitethernet0/1)# no storm-control multicast
Device3(config-if-gigabitethernet0/1)# no spanning-tree enable
Device3(config-if-gigabitethernet0/1)#exit
Device3(config)# interface gigabitethernet 0/2
Device3(config-if-gigabitethernet0/1)# switchport mode trunk
Device3(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device3(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device3(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 3,300-400
Device3(config-if-gigabitethernet0/1)# no storm-control unicast
Device3(config-if-gigabitethernet0/1)# no storm-control broadcast
Device3(config-if-gigabitethernet0/1)# no storm-control multicast
Device3(config-if-gigabitethernet0/1)# no spanning-tree enable
Device3(config-if-gigabitethernet0/1)#end
```

#On Device4, create VLAN2~VLAN3, VLAN100~VLAN200 and VLAN300~VLAN400, configure the link type of ports gigabitethernet0/1 and gigabitethernet0/2 as Trunk, permitting services of VLAN2~VLAN3, VLAN100~VLAN200 and VLAN300~VLAN400 to pass, and disable the spanning tree and storm suppression under the port.

```
Device4#configure terminal
Device4(config)# vlan 2-3,100-200,300-400
Device4(config)# interface gigabitethernet 0/1
Device4(config-if-gigabitethernet0/1)#shutdown
Device4(config-if-gigabitethernet0/1)# switchport mode trunk
Device4(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device4(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device4(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 3,300-400
Device4(config-if-gigabitethernet0/1)# no storm-control unicast
Device4(config-if-gigabitethernet0/1)# no storm-control broadcast
Device4(config-if-gigabitethernet0/1)# no storm-control multicast
Device4(config-if-gigabitethernet0/1)# no spanning-tree enable
Device4(config-if-gigabitethernet0/1)#exit
Device4(config)# interface gigabitethernet 0/2
Device4(config-if-gigabitethernet0/1)# switchport mode trunk
Device4(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device4(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device4(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 3,300-400
Device4(config-if-gigabitethernet0/1)# no storm-control unicast
Device4(config-if-gigabitethernet0/1)# no storm-control broadcast
Device4(config-if-gigabitethernet0/1)# no storm-control multicast
Device4(config-if-gigabitethernet0/1)# no spanning-tree enable
Device4(config-if-gigabitethernet0/1)#end
```

Step 2: Configure MST instance.

#On Device1, configure MST instance 1 to map vlan100-200 and MST instance 2 to map vlan300-400, and activate the instance.

```
Device1#configure terminal
Device1(config)# spanning-tree mst configuration
Device1(config-mst)# instance 1 vlan 100-200
Device1(config-mst)# instance 2 vlan 300-400
Device1(config-mst)# active configuration pending
Device1(config-mst)#end
```

#On Device2, configure MST instance 1 to map vlan100-200 and MST instance 2 to map vlan300-400, and activate the instance.

```
Device2#configure terminal
Device2(config)# spanning-tree mst configuration
Device2(config-mst)# instance 1 vlan 100-200
Device2(config-mst)# instance 2 vlan 300-400
Device2(config-mst)# active configuration pending
Device2(config-mst)#end
```

#On Device3, configure MST instance 1 to map vlan100-200 and MST instance 2 to map vlan300-400, and activate the instance.

```
Device3#configure terminal
Device3(config)# spanning-tree mst configuration
Device3(config-mst)# instance 1 vlan 100-200
Device3(config-mst)# instance 2 vlan 300-400
Device3(config-mst)# active configuration pending
Device3(config-mst)#end
```

#On Device4, configure MST instance 1 to map vlan100-200 and MST instance 2 to map vlan300-400, and activate the instance.

```
Device4#configure terminal
Device4(config)# spanning-tree mst configuration
Device4(config-mst)# instance 1 vlan 100-200
Device4(config-mst)# instance 2 vlan 300-400
Device4(config-mst)# active configuration pending
Device4(config-mst)#end
```

### Step 3: Configure ERPS.

#On Device1, configure ERPS ring1. Configure vlan2 as the control vlan of ring1, gigabitethernet0/1 as the normal port of ring1, gigabitethernet0/2 as the normal port of ring1, and instance 1 as the data vlan of ring1; enable the ERPS function of ring1.

```
Device1# configure terminal
Device1(config)#erps ring 1
Device1(config-erps1)# control vlan 2
Device1(config-erps1)# port0 interface g0/1
Device1(config-erps1)# port1 interface g0/2
Device1(config-erps1)# instance 1
Device1(config-erps1)# erps enable
Device1(config-erps1)# end
```

#On Device1, configure ERPS ring2. Configure vlan3 as the control vlan of ring2, gigabitethernet0/1 as the normal port of ring2, gigabitethernet0/2 as the normal port of ring2, and instance 2 as the data vlan of ring2; enable the ERPS function of ring2.

```
Device1# configure terminal
Device1(config)#erps ring 2
Device1(config-erps1)# control vlan 3
Device1(config-erps1)# port0 interface g0/1
Device1(config-erps1)# port1 interface g0/2
Device1(config-erps1)# instance 2
Device1(config-erps1)# erps enable
Device1(config-erps1)# exit
Device1(config)# interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#no shutdown
Device1(config-if-gigabitethernet0/1)# end
```

#On Device2, configure ERPS ring1. Configure vlan2 as the control vlan of ring1, gigabitethernet0/1 as the owner port of ring1, gigabitethernet0/2 as the normal port of ring1, and instance 1 as the data vlan of ring1; enable the ERPS function of ring1.

```
Device2# configure terminal
Device2(config)#erps ring 1
Device2(config-erps1)# control vlan 2
Device2(config-erps1)# port0 interface g0/1 rpl owner
Device2(config-erps1)# port1 interface g0/2
Device2(config-erps1)# instance 1
Device2(config-erps1)# erps enable
Device2(config-erps1)# exit
```

#On Device2, configure ERPS ring2. Configure vlan3 as the control vlan of ring2, gigabitethernet0/1 as the neighbor port of ring2, gigabitethernet0/2 as the normal port of ring2, and instance 2 as the data vlan of ring2; enable the ERPS function of ring2.

```
Device2# configure terminal
Device2(config)#erps ring 2
Device2(config-erps1)# control vlan 3
Device2(config-erps1)# port0 interface g0/1 rpl neighbor
Device2(config-erps1)# port1 interface g0/2
Device2(config-erps1)# instance 2
Device2(config-erps1)# erps enable
Device2(config-erps1)# exit
Device2(config)# interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#no shutdown
Device2(config-if-gigabitethernet0/1)# end
```

#On Device3, configure ERPS ring1. Configure vlan2 as the control vlan of ring1, gigabitethernet0/1 as the normal port of ring1, gigabitethernet0/2 as the normal port of ring1, and instance 1 as the data vlan of ring1; enable the ERPS function of ring1.

```
Device3# configure terminal
Device3(config)#erps ring 1
Device3(config-erps1)# control vlan 2
Device3(config-erps1)# port0 interface g0/1
Device3(config-erps1)# port1 interface g0/2
Device3(config-erps1)# instance 1
Device3(config-erps1)# erps enable
Device3(config-erps1)# exit
```

#On Device3, configure ERPS ring2. Configure vlan3 as the control vlan of ring2, gigabitethernet0/1 as the normal port of ring2, gigabitethernet0/2 as the normal port of ring2, and instance 2 as the data vlan of ring2; enable the ERPS function of ring2.

```
Device3# configure terminal
Device3(config)#erps ring 2
```

```

Device3(config-erps1)# control vlan 3
Device3(config-erps1)# port0 interface g0/1
Device3(config-erps1)# port1 interface g0/2
Device3(config-erps1)# instance 2
Device3(config-erps1)# erps enable
Device3(config-erps1)# exit
Device3(config)# interface gigabitethernet 0/1
Device3(config-if-gigabitethernet0/1)#no shutdown
Device3(config-if-gigabitethernet0/1)# end

```

#On Device4, configure ERPS ring1. Configure vlan2 as the control vlan of ring1, gigabitethernet0/1 as the normal port of ring1, gigabitethernet0/2 as the neighbor port of ring1, and instance 1 as the data vlan of ring1; enable the ERPS function of ring1.

```

Device4# configure terminal
Device4(config)#erps ring 1
Device4(config-erps1)# control vlan 2
Device4(config-erps1)# port0 interface g0/1
Device4(config-erps1)# port1 interface g0/2 rpl neighbour
Device4(config-erps1)# instance 1
Device4(config-erps1)# erps enable
Device4(config-erps1)# exit

```

#On Device4, configure ERPS ring2. Configure vlan3 as the control vlan of ring2, gigabitethernet0/1 as the normal port of ring2, gigabitethernet0/2 as the owner port of ring2, and instance 2 as the data vlan of ring2; enable the ERPS function of ring2.

```

Device4# configure terminal
Device4(config)#erps ring 2
Device4(config-erps1)# control vlan 3
Device4(config-erps1)# port0 interface g0/1
Device4(config-erps1)# port1 interface g0/2 rpl owner
Device4(config-erps1)# instance 2
Device4(config-erps1)# erps enable
Device4(config-erps1)# exit
Device4(config)# interface gigabitethernet 0/1
Device4(config-if-gigabitethernet0/1)#no shutdown
Device4(config-if-gigabitethernet0/1)# end

```

Step 4: Check the result.

#After the network topology is stable, check the ERPS information of the Device. Take Device2 as an example.

#View the ERPS information of Device2.

```

Device2# show erps ring 1 detail
Ring ID      : 1
Version      : v2
R-APS mel    : 7
Instance     : 1 vlans mapped : 100-200
Control VLAN : 2
Node role    : Owner
Node state   : idle
Guard timer  : 500 ms      Running : 0 ms
Holdoff timer : 0 ms      Running : 0 ms
WTR timer    : 5 min      Running : 0 s
WTB timer    : 7 s        Running : 0 s
Subring      : No
Tc-limit enable : No
Tc-limit Interval : 2

```

Tc-limit Threshold : 3  
 Revertive operation : Revertive  
 R-APS channel : Non-Virtual channel  
 Enable status : Enable  
 Gigabitethernet0/1 Flush Logic  
 Remote Node ID : 0000-0000-0000  
 Remote BPR : 0  
 Gigabitethernet0/1 track CFM  
 MD Name :  
 MA Name :  
 MEP ID : 0  
 RMEP ID : 0  
 CFM State : 0  
 Gigabitethernet0/2 Flush Logic  
 Remote Node ID : 0000-0000-0000  
 Remote BPR : 0  
 Gigabitethernet0/2 track CFM  
 MD Name :  
 MA Name :  
 MEP ID : 0  
 RMEP ID : 0  
 CFM State : 0

Port	Name	PortRole	SwitchType	PortStatus	SignalStatus
Port0	gigabitethernet0/1	Owner	--	Blocking	Non-failed
Port1	gigabitethernet0/2	Normal	--	Forwarding	Non-failed

Device2# show erps ring 2 detail

Ring ID : 2  
 Version : v2  
 R-APS mel : 7  
 Instance : 2 vlans mapped : 300-400  
 Control VLAN : 3  
 Node role : Neighbour  
 Node state : idle  
 Guard timer : 500 ms Running : 0 ms  
 Holdoff timer : 0 ms Running : 0 ms  
 WTR timer : 5 min Running : 0 s  
 WTB timer : 7 s Running : 0 s  
 Subring : No  
 Tc-limit enable : No  
 Tc-limit Interval : 2  
 Tc-limit Threshold : 3  
 Revertive operation : Revertive  
 R-APS channel : Non-Virtual channel  
 Enable status : Enable  
 Gigabitethernet0/1 Flush Logic  
 Remote Node ID : 0000-0000-0000  
 Remote BPR : 0  
 Gigabitethernet0/1 track CFM  
 MD Name :  
 MA Name :  
 MEP ID : 0  
 RMEP ID : 0  
 CFM State : 0  
 Gigabitethernet0/2 Flush Logic  
 Remote Node ID : 0000-0000-0000  
 Remote BPR : 0  
 Gigabitethernet0/2 track CFM  
 MD Name :  
 MA Name :  
 MEP ID : 0  
 RMEP ID : 0

CFM State : 0

Port	Name	PortRole	SwitchType	PortStatus	SignalStatus
Port0	gigabitethernet0/1	Neighbour	--	Blocking	Non-failed
Port1	gigabitethernet0/2	Normal	--	Forwarding	Non-failed

## Note

- When loading, the logical rings on the same physical ring cannot be configured with the same data instance.

### 110.3.3 Configure ERPS Intersecting Rings

#### Network Requirements

- All devices are within the same layer-2 network.
- Device1-Device2-Device4-Device3 and Device3-Device5-Device6-Device4 form two physical loops respectively. ERPS is enabled on all Devices to disconnect the link loop.

#### Network Topology

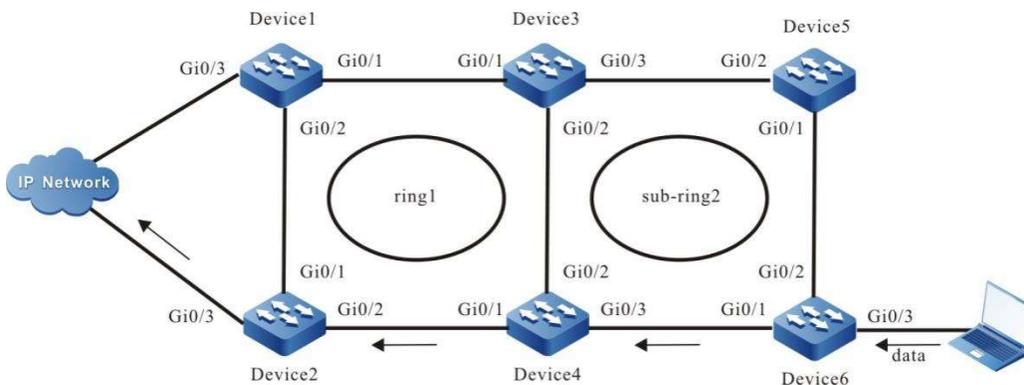


Figure 110 Configuring ERPS Intersecting Rings

#### Configuration Steps

Step 1: Configure VLANs, and configure the link type of the ports.

#On Device1, create VLAN2 and VLAN100~VLAN200, configure the link type of ports gigabitethernet0/1 and gigabitethernet0/2 as Trunk, permitting services of VLAN2 and VLAN100~VLAN200 to pass, and disable the spanning tree and storm suppression under the port.

```
Device1#configure terminal
Device1(config)#vlan 2,100-200
```

```

Device1(config)# interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#shutdown
Device1(config-if-gigabitethernet0/1)# switchport mode trunk
Device1(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device1(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device1(config-if-gigabitethernet0/1)# no storm-control unicast
Device1(config-if-gigabitethernet0/1)# no storm-control broadcast
Device1(config-if-gigabitethernet0/1)# no storm-control multicast
Device1(config-if-gigabitethernet0/1)# no spanning-tree enable
Device1(config-if-gigabitethernet0/1)#exit
Device1(config)# interface gigabitethernet 0/2
Device1(config-if-gigabitethernet0/1)# switchport mode trunk
Device1(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device1(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device1(config-if-gigabitethernet0/1)# no storm-control unicast
Device1(config-if-gigabitethernet0/1)# no storm-control broadcast
Device1(config-if-gigabitethernet0/1)# no storm-control multicast
Device1(config-if-gigabitethernet0/1)# no spanning-tree enable
Device1(config-if-gigabitethernet0/1)#end

```

#On Device2, create VLAN2 and VLAN100~VLAN200, configure the link type of ports gigabitethernet0/1 and gigabitethernet0/2 as Trunk, permitting services of VLAN2 and VLAN100~VLAN200 to pass, and disable the spanning tree and storm suppression under the port.

```

Device2#configure terminal
Device2(config)#vlan 2,100-200
Device2(config)# interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#shutdown
Device2(config-if-gigabitethernet0/1)# switchport mode trunk
Device2(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device2(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device2(config-if-gigabitethernet0/1)# no storm-control unicast
Device2(config-if-gigabitethernet0/1)# no storm-control broadcast
Device2(config-if-gigabitethernet0/1)# no storm-control multicast
Device2(config-if-gigabitethernet0/1)# no spanning-tree enable
Device2(config-if-gigabitethernet0/1)#exit
Device2(config)# interface gigabitethernet 0/2
Device2(config-if-gigabitethernet0/1)# switchport mode trunk
Device2(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device2(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device2(config-if-gigabitethernet0/1)# no storm-control unicast
Device2(config-if-gigabitethernet0/1)# no storm-control broadcast
Device2(config-if-gigabitethernet0/1)# no storm-control multicast
Device2(config-if-gigabitethernet0/1)# no spanning-tree enable
Device2(config-if-gigabitethernet0/1)#end

```

#On Device3, create VLAN2~VLAN3 and VLAN100~VLAN200, configure the link type of ports gigabitethernet0/1 and gigabitethernet0/2 as Trunk, permitting services of VLAN2 and VLAN100~VLAN200 to pass; configure the link type of port gigabitethernet0/3 as Trunk, permitting services of VLAN3 and VLAN100~VLAN200, and disable the spanning tree and storm suppression under the port.

```

Device3#configure terminal
Device3(config)#vlan 2-3,100-200
Device3(config)# interface gigabitethernet 0/1
Device3(config-if-gigabitethernet0/1)#shutdown
Device3(config-if-gigabitethernet0/1)# switchport mode trunk
Device3(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device3(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device3(config-if-gigabitethernet0/1)# no storm-control unicast
Device3(config-if-gigabitethernet0/1)# no storm-control broadcast

```

```

Device3(config-if-gigabitethernet0/1)# no storm-control multicast
Device3(config-if-gigabitethernet0/1)# no spanning-tree enable
Device3(config-if-gigabitethernet0/1)#exit
Device3(config)# interface gigabitethernet 0/2
Device3(config-if-gigabitethernet0/1)# switchport mode trunk
Device3(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device3(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device3(config-if-gigabitethernet0/1)# no storm-control unicast
Device3(config-if-gigabitethernet0/1)# no storm-control broadcast
Device3(config-if-gigabitethernet0/1)# no storm-control multicast
Device3(config-if-gigabitethernet0/1)# no spanning-tree enable
Device3(config-if-gigabitethernet0/1)#end
Device3(config)# interface gigabitethernet 0/3
Device3(config-if-gigabitethernet0/1)#shutdown
Device3(config-if-gigabitethernet0/1)# switchport mode trunk
Device3(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device3(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 3,100-200
Device3(config-if-gigabitethernet0/1)# no storm-control unicast
Device3(config-if-gigabitethernet0/1)# no storm-control broadcast
Device3(config-if-gigabitethernet0/1)# no storm-control multicast
Device3(config-if-gigabitethernet0/1)# no spanning-tree enable
Device3(config-if-gigabitethernet0/1)#exit

```

#On Device4, create VLAN2~VLAN3 and VLAN100~VLAN200, configure the link type of ports gigabitethernet0/1 and gigabitethernet0/2 as Trunk, permitting services of VLAN2 and VLAN100~VLAN200 to pass; configure the link type of port gigabitethernet0/3 as Trunk, permitting services of VLAN3 and VLAN100~VLAN200, and disable the spanning tree and storm suppression under the port.

```

Device4#configure terminal
Device4(config)#vlan 2-3,100-200
Device4(config)# interface gigabitethernet 0/1
Device4(config-if-gigabitethernet0/1)#shutdown
Device4(config-if-gigabitethernet0/1)# switchport mode trunk
Device4(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device4(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device4(config-if-gigabitethernet0/1)# no storm-control unicast
Device4(config-if-gigabitethernet0/1)# no storm-control broadcast
Device4(config-if-gigabitethernet0/1)# no storm-control multicast
Device4(config-if-gigabitethernet0/1)# no spanning-tree enable
Device4(config-if-gigabitethernet0/1)#exit
Device4(config)# interface gigabitethernet 0/2
Device4(config-if-gigabitethernet0/1)# switchport mode trunk
Device4(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device4(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device4(config-if-gigabitethernet0/1)# no storm-control unicast
Device4(config-if-gigabitethernet0/1)# no storm-control broadcast
Device4(config-if-gigabitethernet0/1)# no storm-control multicast
Device4(config-if-gigabitethernet0/1)# no spanning-tree enable
Device4(config-if-gigabitethernet0/1)#end
Device4(config)# interface gigabitethernet 0/3
Device4(config-if-gigabitethernet0/1)#shutdown
Device4(config-if-gigabitethernet0/1)# switchport mode trunk
Device4(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device4(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 3,100-200
Device4(config-if-gigabitethernet0/1)# no storm-control unicast
Device4(config-if-gigabitethernet0/1)# no storm-control broadcast
Device4(config-if-gigabitethernet0/1)# no storm-control multicast
Device4(config-if-gigabitethernet0/1)# no spanning-tree enable
Device4(config-if-gigabitethernet0/1)#exit

```

#On Device5, create VLAN3 and VLAN100~VLAN200, configure the link type of ports gigabitethernet0/1 and gigabitethernet0/2 as Trunk, permitting services of VLAN3 and VLAN100~VLAN200 to pass, and disable the spanning tree and storm suppression under the port.

```
Device5#configure terminal
Device5(config)#vlan 3,100-200
Device5(config)# interface gigabitethernet 0/1
Device5(config-if-gigabitethernet0/1)#shutdown
Device5(config-if-gigabitethernet0/1)# switchport mode trunk
Device5(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device5(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 3,100-200
Device5(config-if-gigabitethernet0/1)# no storm-control unicast
Device5(config-if-gigabitethernet0/1)# no storm-control broadcast
Device5(config-if-gigabitethernet0/1)# no storm-control multicast
Device5(config-if-gigabitethernet0/1)# no spanning-tree enable
Device5(config-if-gigabitethernet0/1)#exit
Device5(config)# interface gigabitethernet 0/2
Device5(config-if-gigabitethernet0/1)# switchport mode trunk
Device5(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device5(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 3,100-200
Device5(config-if-gigabitethernet0/1)# no storm-control unicast
Device5(config-if-gigabitethernet0/1)# no storm-control broadcast
Device5(config-if-gigabitethernet0/1)# no storm-control multicast
Device5(config-if-gigabitethernet0/1)# no spanning-tree enable
Device5(config-if-gigabitethernet0/1)#end
```

#On Device6, create VLAN3 and VLAN100~VLAN200, configure the link type of ports gigabitethernet0/1 and gigabitethernet0/2 as Trunk, permitting services of VLAN3 and VLAN100~VLAN200 to pass, and disable the spanning tree and storm suppression under the port.

```
Device3#configure terminal
Device3(config)#vlan 3,100-200
Device3(config)# interface gigabitethernet 0/1
Device3(config-if-gigabitethernet0/1)#shutdown
Device3(config-if-gigabitethernet0/1)# switchport mode trunk
Device3(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device3(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 3,100-200
Device3(config-if-gigabitethernet0/1)# no storm-control unicast
Device3(config-if-gigabitethernet0/1)# no storm-control broadcast
Device3(config-if-gigabitethernet0/1)# no storm-control multicast
Device3(config-if-gigabitethernet0/1)# no spanning-tree enable
Device3(config-if-gigabitethernet0/1)#exit
Device3(config)# interface gigabitethernet 0/2
Device3(config-if-gigabitethernet0/1)# switchport mode trunk
Device3(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device3(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 3,100-200
Device3(config-if-gigabitethernet0/1)# no storm-control unicast
Device3(config-if-gigabitethernet0/1)# no storm-control broadcast
Device3(config-if-gigabitethernet0/1)# no storm-control multicast
Device3(config-if-gigabitethernet0/1)# no spanning-tree enable
Device3(config-if-gigabitethernet0/1)#end
```

Step 2: Configure MST instance.

#On Device1, configure MST instance 1 to map vlan100-200, and activate the instance.

```
Device1#configure terminal
Device1(config)# spanning-tree mst configuration
Device1(config-mst)# instance 1 vlan 100-200
Device1(config-mst)# active configuration pending
```

```
Device1(config-mst)#end
```

#On Device2, configure MST instance 1 to map vlan100-200, and activate the instance.

```
Device2#configure terminal
Device2(config)# spanning-tree mst configuration
Device2(config-mst)# instance 1 vlan 100-200
Device2(config-mst)# active configuration pending
Device2(config-mst)#end
```

#On Device3, configure MST instance 1 to map vlan100-200, and activate the instance.

```
Device3#configure terminal
Device3(config)# spanning-tree mst configuration
Device3(config-mst)# instance 1 vlan 100-200
Device3(config-mst)# active configuration pending
Device3(config-mst)#end
```

#On Device4, configure MST instance 1 to map vlan100-200, and activate the instance.

```
Device4#configure terminal
Device4(config)# spanning-tree mst configuration
Device4(config-mst)# instance 1 vlan 100-200
Device4(config-mst)# active configuration pending
Device4(config-mst)#end
```

#On Device5, configure MST instance 1 to map vlan100-200, and activate the instance.

```
Device5#configure terminal
Device5(config)# spanning-tree mst configuration
Device5(config-mst)# instance 1 vlan 100-200
Device5(config-mst)# active configuration pending
Device5(config-mst)#end
```

#On Device6, configure MST instance 1 to map vlan100-200, and activate the instance.

```
Device6#configure terminal
Device6(config)# spanning-tree mst configuration
Device6(config-mst)# instance 1 vlan 100-200
Device6(config-mst)# active configuration pending
Device6(config-mst)#end
```

### Step 3: Configure ERPS.

#On Device1, configure ERPS ring1. Configure vlan2 as the control vlan of ring1, gigabitethernet0/1 as the normal port of ring1, gigabitethernet0/2 as the owner port of ring1, and instance 1 as the data vlan of ring1; enable the ERPS function of ring1.

```
Device1# configure terminal
Device1 (config)#erps ring 1
Device1 (config-erps1)# control vlan 2
Device1 (config-erps1)# port0 interface g0/1
Device1 (config-erps1)# port1 interface g0/2 rpl owner
Device1 (config-erps1)# instance 1
Device1 (config-erps1)# erps enable
Device1 (config-erps1)# end
Device1 (config)# interface gigabitethernet 0/1
Device1 (config-if-gigabitethernet0/1)#no shutdown
Device1 (config-if-gigabitethernet0/1)# end
```

#On Device2, configure ERPS ring1. Configure vlan2 as the control vlan of ring1, gigabitethernet0/1 as the neighbor port of ring1, gigabitethernet0/2 as the normal port of ring1, and instance 1 as the data vlan of ring1; enable the ERPS function of ring1.

```
Device2# configure terminal
Device2(config)#erps ring 1
Device2(config-erps1)# control vlan 2
Device2(config-erps1)# port0 interface g0/1 rpl neighbour
Device2(config-erps1)# port1 interface g0/2
Device2(config-erps1)# instance 1
Device2(config-erps1)# erps enable
Device2(config-erps1)# exit
Device2(config)# interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#no shutdown
Device2(config-if-gigabitethernet0/1)# end
```

#On Device3, configure ERPS ring1. Configure vlan2 as the control vlan of ring1, gigabitethernet0/1 as the normal port of ring1, gigabitethernet0/2 as the normal port of ring1, and instance 1 as the data vlan of ring1; enable the ERPS function of ring1.

```
Device3# configure terminal
Device3(config)#erps ring 1
Device3(config-erps1)# control vlan 2
Device3(config-erps1)# port0 interface g0/1
Device3(config-erps1)# port1 interface g0/2
Device3(config-erps1)# instance 1
Device3(config-erps1)# erps enable
Device3(config-erps1)# exit
Device2(config)# interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#no shutdown
Device2(config-if-gigabitethernet0/1)# end
```

#On Device3, configure ERPS ring2. Configure vlan3 as the control vlan of ring2, gigabitethernet0/3 as the normal port of ring2, instance 1 as the data vlan of ring2, and ring2 as a subring; enable the ERPS function of ring2.

```
Device3# configure terminal
Device3(config)#erps ring 2
Device3(config-erps1)# control vlan 3
Device3(config-erps1)# port0 interface g0/3
Device3(config-erps1)# instance 1
Device3(config-erps1)# sub-ring
Device3(config-erps1)# erps enable
Device3(config-erps1)# exit
Device3(config)# interface gigabitethernet 0/3
Device3(config-if-gigabitethernet0/1)#no shutdown
Device3(config-if-gigabitethernet0/1)# end
```

#On Device4, configure ERPS ring1. Configure vlan2 as the control vlan of ring1, gigabitethernet0/1 as the normal port of ring1, gigabitethernet0/2 as the normal port of ring1, and instance 1 as the data vlan of ring1; enable the ERPS function of ring1.

```
Device4# configure terminal
Device4(config)#erps ring 1
Device4(config-erps1)# control vlan 2
Device4(config-erps1)# port0 interface g0/1
Device4(config-erps1)# port1 interface g0/2
Device4(config-erps1)# instance 1
Device4(config-erps1)# erps enable
Device4(config-erps1)# exit
```

```
Device4(config)# interface gigabitethernet 0/1
Device4(config-if-gigabitethernet0/1)#no shutdown
Device4(config-if-gigabitethernet0/1)# end
```

#On Device4, configure ERPS ring2. Configure vlan3 as the control vlan of ring2, gigabitethernet0/3 as the normal port of ring2, instance 1 as the data vlan of ring2, and ring2 as a subring; enable the ERPS function of ring2.

```
Device4# configure terminal
Device4(config)#erps ring 2
Device4(config-erps1)# control vlan 3
Device4(config-erps1)# port0 interface g0/3
Device4(config-erps1)# instance 1
Device4(config-erps1)# sub-ring
Device4(config-erps1)# erps enable
Device4(config-erps1)# exit
Device4(config)# interface gigabitethernet 0/3
Device4(config-if-gigabitethernet0/1)#no shutdown
Device4(config-if-gigabitethernet0/1)# end
```

#On Device5, configure ERPS ring2. Configure vlan3 as the control vlan of ring2, gigabitethernet0/2 as the normal port of ring2, gigabitethernet0/1 as the owner port of ring2, instance 1 as the data vlan of ring2, and ring2 as a subring; enable the ERPS function of ring2.

```
Device4# configure terminal
Device4(config)#erps ring 2
Device4(config-erps1)# control vlan 3
Device4(config-erps1)# port0 interface g0/1 rpl owner
Device4(config-erps1)# port0 interface g0/2
Device4(config-erps1)# instance 1
Device4(config-erps1)# sub-ring
Device4(config-erps1)# erps enable
Device4(config-erps1)# exit
Device4(config)# interface gigabitethernet 0/1
Device4(config-if-gigabitethernet0/1)#no shutdown
Device4(config-if-gigabitethernet0/1)# end
```

#On Device6, configure ERPS ring2. Configure vlan3 as the control vlan of ring2, gigabitethernet0/2 as the neighbor port of ring2, gigabitethernet0/1 as the normal port of ring2, instance 1 as the data vlan of ring2, and ring2 as a subring; enable the ERPS function of ring2.

```
Device4# configure terminal
Device4(config)#erps ring 2
Device4(config-erps1)# control vlan 3
Device4(config-erps1)# port0 interface g0/1
Device4(config-erps1)# port0 interface g0/2 rpl neighbour
Device4(config-erps1)# instance 1
Device4(config-erps1)# sub-ring
Device4(config-erps1)# erps enable
Device4(config-erps1)# exit
Device4(config)# interface gigabitethernet 0/1
Device4(config-if-gigabitethernet0/1)#no shutdown
Device4(config-if-gigabitethernet0/1)# end
```

Step 4: Check the result.

#After the network topology is stable, check the ERPS information of the Device. Take Device3 as an example.

#View the ERPS information of Device3.

```

Device3# show erps ring 1 detail
Ring ID      : 1
Version      : v2
R-APS mel    : 7
Instance     : 1 vlans mapped : 100-200
Control VLAN : 2
Node role    : Normal
Node state   : idle
Guard timer  : 500 ms      Running : 0 ms
Holdoff timer : 0 ms      Running : 0 ms
WTR timer    : 5 min      Running : 0 s
WTB timer    : 7 s        Running : 0 s
Subring      : No
Tc-limit enable : No
Tc-limit Interval : 2
Tc-limit Threshold : 3
Revertive operation : Revertive
R-APS channel : Non-Virtual channel
Enable status : Enable
Gigabitethernet0/1 Flush Logic
  Remote Node ID : 0000-0000-0000
  Remote BPR     : 0
Gigabitethernet0/1 track CFM
  MD Name        :
  MA Name        :
  MEP ID         : 0
  RMEP ID        : 0
  CFM State      : 0
Gigabitethernet0/2 Flush Logic
  Remote Node ID : 0000-0000-0000
  Remote BPR     : 0
Gigabitethernet0/2 track CFM
  MD Name        :
  MA Name        :
  MEP ID         : 0
  RMEP ID        : 0
  CFM State      : 0

```

Port	Name	PortRole	SwitchType	PortStatus	SignalStatus
Port0	gigabitethernet0/1	Normal	--	Forwarding	Non-failed
Port1	gigabitethernet0/2	Normal	--	Forwarding	Non-failed

```

Device3# show erps ring 2 detail
Ring ID      : 2
Version      : v2
R-APS mel    : 7
Instance     : 1 vlans mapped : 100-200
Control VLAN : 3
Node role    : Normal
Node state   : idle
Guard timer  : 500 ms      Running : 0 ms
Holdoff timer : 0 ms      Running : 0 ms
WTR timer    : 5 min      Running : 0 s
WTB timer    : 7 s        Running : 0 s
Subring      : No
Tc-limit enable : No
Tc-limit Interval : 2
Tc-limit Threshold : 3
Revertive operation : Revertive
R-APS channel : Non-Virtual channel
Enable status : Enable

```

```

Gigabitethernet0/3 Flush Logic
  Remote Node ID : 0000-0000-0000
  Remote BPR   : 0
Gigabitethernet0/1 track CFM
  MD Name   :
  MA Name   :
  MEP ID    : 0
  RMEP ID   : 0
  CFM State : 0
Port  Name                PortRole  SwitchType  PortStatus  SignalStatus
-----
Port0  gigabitethernet0/3  Normal    --         Forwarding  Non-failed

```

# 111 Network Test and Fault Diagnosis

---

## 111.1 Overview

With the network test and fault diagnosis tool, we can check the network connection status and diagnose the system fault. In daily maintenance, when it is necessary to check the network connection, we can use the ping function and traceroute function. When it is necessary to diagnose the system fault, we can open the system debugging information to diagnose the system fault.

## 111.2 Network Test and Fault Diagnosis Application

Table 111-1 Application List of Network Test and Fault Diagnosis

Application functions	
Ping function	ping
	ping ip
	Interactive ping
	grouping
Traceroute function	traceroute
	Interactive traceroute
System debugging function	System debugging

### 111.2.1 Ping Function

The ping function is used to check the network connection status and the availability of hosts. The ping function sends the ICMP echo request packet to the host and waits for the ICMP echo response, used to judge whether the destination is reachable. ping can also measure the round trip time from the source to the destination.

#### Configuration Condition

None

#### ping

Table 111-2 Ping

Step	Command	Description
Check whether the specified destination address is reachable	<b>ping</b> [ <b>vrf</b> <i>vrf-name</i> ] { [ <b>ip</b> <i>host-name</i> / <i>ip-address</i> ] / [ <b>ipv6</b> <i>host-name</i> / <i>ipv6-address</i> ]   <i>host-name</i> / <i>ip-address</i>   <i>ipv6-address</i> } [ <b>-l</b> <i>packet-length</i> ] [ <b>-w</b> <i>wait-time</i> ] [ <b>-n</b> <i>packet-number</i> / <b>-t</b> ]	Mandatory

## Interactive Ping

If you need to use options such as loose source routing options, strict source routing options, logging routes, logging timestamps, or need to know the maximum ICMP packet size supported by the peer device, you can use interactive ping to achieve this.

Table 3-111 Interactive Ping

Step	Command	Description
Enter the interactive ping mode.	<b>ping</b> [ vrf <i>vrf-name</i> ]	Mandatory  Execute this command in privileged user mode to enter ping interactive mode.
Configure Network Protocol Types	<b>Protocol</b> [ ip ]: [ ip   ipv6 ]	Optional  By default, the IPv4 protocol is used.
Configure the destination IP address or host name.	<b>Target IP address or hostname:</b> { <i>ip-address</i>   <i>host-name</i> }	Mandatory
Configure the number of attempts to send ICMP request packet.	<b>Repeat count</b> [5]: [ <i>repeat-count</i> ]	Optional  By default, the number is 5.
Configure the length of the ICMP request packet.	<b>Datagram size</b> [76]: [ <i>datagram-size</i> ]	Optional  The length of the packet is the length of the entire IP packet.  By default, the packet length is 76 bytes.
Configure the timeout time for ICMP responses.	<b>Timeout in seconds</b> [2]: [ <i>timeout</i> ]	Optional  By default, the timeout is 2 seconds.

Step	Command	Description
Enable extended options.	<b>Extended commands</b> [no]: [ yes / no ]	Optional  The configuration commands for the extended options are visible only after the extended options are enabled.  By default, the extension option is not enabled.
Configure the extended option, source IP address or output interface for ICMP request packets.	<b>Source address or interface:</b> { <i>ip-address / interfacename</i> }	Optional  The command can only be configured if the extended option is enabled.  By default, the source address and output interface of the request packets are not specified.
Configure extended selection, service type of ICMP request packet.	<b>Type of service [0]:</b> [ <i>tos</i> ]	Optional. This command is supported only for IPv4 protocol.  The command can only be configured after the extended option is enabled.  By default, the TOS value is 0.
Configure extended options to ban reassembly.	<b>Set DF bit in IP header?</b> [ no ]: [ yes / no ]	Optional. This command is supported only for IPv4 protocol.  The command can only be configured after the

Step	Command	Description
		<p>extended option is enabled.</p> <p>By default, no DF flag is set and reassembly is permitted.</p>
<p>Configure extended options to verify the data content of the response packet.</p>	<p><b>Validate reply data?</b> [ no ]: [ yes / no ]</p>	<p>Optional. This command is supported only for IPv4 protocol.</p> <p>The command can only be configured after the extended option is enabled.</p> <p>By default, no data content is verified.</p>
<p>Configure extended options to enable ICMP request data content of the packet.</p>	<p><b>Data pattern [abcd]:</b> [ <i>data-pattern</i> ]</p>	<p>Optional</p> <p>The command can only be configured after the extended option is enabled.</p> <p>By default, the data content template is set as "abcd".</p>
<p>Configure extended options, loose source routing options, strict source routing options, logging routes, logging timestamps, and display details.</p>	<p><b>Loose, Strict, Record, Timestamp,</b> <b>Verbose[ none ]:</b> [ l   s ] [ r / t / v ]</p>	<p>Optional. This command is supported only for IPv4 protocol.</p> <p>The command can only be configured after the extended option is enabled.</p> <p>By default, the extended option is not configured.</p>

Step	Command	Description
Enable sweep of the ICMP request packet.	<b>Sweep range of sizes</b> [ no ]: [ yes / no ]	Optional. This command is supported only for IPv4 protocol.  By default, the sweep option is disabled.
Configure the sweep start value.	<b>Sweep min size [36]:</b> [ <i>min-size</i> ]	Optional. This command is supported only for IPv4 protocol.  This command can only be configured after sweep is enabled.  By default, the sweep start value is 36.
Configure sweep end value.	<b>Sweep max size</b> [18024]: [ <i>max-size</i> ]	Optional. This command is supported only for IPv4 protocol.  This command can only be configured after sweep is enabled.  By default, the end value of sweep is 18024.
Configure sweep increment.	<b>Sweep interval [1]:</b> [ <i>interval</i> ]	Optional. This command is supported only for IPv4 protocol.  This command can only be configured after sweep is enabled.  By default, the sweep increment is 1.

The device supports sending multiple ICMP echo requests at once to get a more accurate network connection status based on the number of ICMP reply packets returned by the destination host.

Table 4-5 Grouping

Step	Command	Description
Send multiple ICMP request packets to check if the specified destination address is reachable.	<b>grouping</b> [ <i>vrf vrf-name</i> ] { <i>hostname   ip-address</i> } [ [ -l <i>packet-length</i> ] [ -g <i>packet-group</i> ] [ -w <i>wait-time</i> ] [ -n <i>packet-number</i> ] [ -t ]	Mandatory

### Note

- When pinging the destination host name, first configure the DNS function. Otherwise, ping fails. For DNS configuration, refer to “DNS Configuration” in “IP Network Protocol Configuration”.

## 111.2.2 Traceroute Function

The traceroute function is used to view the gateway through which a packet passes from the source to the destination. It is mainly used to detect whether the destination is reachable and to analyze the faulty network nodes. The executing process of traceroute is: First send one IP packet with TTL 1 to the destination host; the first-hop gateway drops the packet and returns one ICMP timeout error packet. In this way, traceroute gets the first gateway address in the path. And then traceroute sends one packet with TTL 2. In this way, get the address of the second-hop gateway. Continue the process until reaching the destination host. The UDP port number of the traceroute packet is the port number of the destination that cannot be used by any application program. After the destination receives the packet, return one error packet of the port unreachable. In this way, get all gateway addresses on the path.

### Configuration Condition

None

### Traceroute

Table 6-7 Traceroute

Step	Command	Description
View the gateway through which the data packet travels from the source to the destination.	<b>tracert</b> [ <b>vrf vrf-name</b> ] {{ <b>ip</b> <i>host-name</i>   <i>ip-address</i> }   {{ <b>ipv6</b> <i>host-name</i>   <i>ipv6-address</i> }   <i>host-name</i>   <i>ip-address</i>   <i>ipv6-address</i> } [ -f <i>start-ttl</i> ] [ -w <i>wait-time</i> ] [ -m <i>max-ttl</i> ]	Mandatory

## Interactive Traceroute

Table 8-9 Interactive Traceroute

Step	Command	Description
Enter interactive traceroute mode.	<b>tracert</b> [ <b>vrf vrf-name</b> ]	Mandatory  Execute this command in privileged user mode to enter interactive traceroute mode.
Configure Network Protocol Types	<b>Protocol</b> [ <b>ip</b> ]: [ <b>ip</b>   <b>ipv6</b> ]	Optional  By default, the IPv4 protocol is used.
Configure the destination IP address or host name.	<b>Target IP address or hostname:</b> { <i>ip-address</i>   <i>host-name</i> }	Mandatory
Configure the source IP address or output interface for traceroute packets.	<b>Source address or interface:</b> { <i>ip-address</i>   <i>interface-name</i> }	Optional  By default, the source IP address or output interface of the packet is not specified.

Step	Command	Description
Configure the timeout period for each inspection packet response.	<b>Timeout in seconds [3]:</b> <i>timeout</i>	Optional By default, the timeout is 3 seconds.
Configure the number of attempts to send inspection packets with the same TTL value.	<b>Probe count [3]:</b> <i>probe-count</i>	Optional By default, the number is 3.
Configure the minimum TTL value for inspection packets.	<b>Minimum Time to Live [1]:</b> <i>min-ttl</i>	Optional By default, the minimum TTL value is 1.
Configure the maximum TTL value for inspection packets.	<b>Maximum Time to Live [30]:</b> <i>max-ttl</i>	Optional By default, the maximum TTL value is 30.
Configure the destination UDP port number of the inspection packets.	<b>Port Number [33434]:</b> <i>port-number</i>	Optional By default, the destination port number is 33434.
Configure loose source routing options, strict source routing options, logging routes, logging timestamps, and display details.	<b>Loose, Strict, Record, Timestamp, Verbose[ none ]:</b> [ l   s ] [ r / t / v ]	Optional. This command is supported only for IPv4 protocol. By default, the option is not configured.

### 111.2.3 System Debugging Function

To help the user diagnose the problem, the most function modules of the device provide the debugging function.

The debugging function has two switch controls:

- The debugging switch of the module, controlling whether to generate the debugging information of the module
- The output switch of the screen, controlling whether to output the debugging information to the terminal

#### Configuration Condition

None

#### System Debugging

Table 111-10 System Debugging

Step	Command	Description
Turn on the system debugging screen output switch for remote login.	<b>terminal monitor</b>	Optional Remote login includes telnet, ssh and other methods. By default, the switch is off.
Enter the global configuration mode.	<b>configure terminal</b>	-
Turn on the system debugging screen output switch in the console.	<b>logging console</b>	Optional By default, the switch is on.
Exit global configuration mode	<b>exit</b>	-
Turn on the debugging switch of the system function module.	<b>debug { all   module-name [ option ] }</b>	Optional By default, the debugging switches of all functional

Step	Command	Description
		modules of the system are off.

### Note

- The debugging information can be displayed on the terminal only after configuring debug module-name option, terminal monitor or logging console at the same time.
- The generating and output of the debugging information affect the system performance, so when it is necessary, had better use the debug module-name option command to open the specified debugging switch. The debug all command opens all debugging switches, so we had better not use. After debugging ends, close the corresponding debugging switch in time or use the no debug all command to close all debugging switches.

## 111.2.4 Network Test and Fault Diagnosis Monitoring and Maintaining

Table 11-12 System Test and Fault Diagnosis Monitoring and Maintaining

Command	Description
<b>show debugging</b>	Display information about the function modules in the system for which the debugging switch is turned on.

## 111.3 Typical Configuration Example of Network Test and Fault Diagnosis

### 111.3.1 Application of Ping

#### Network Requirements

- Device1 failed to log into Device3 using telnet IP address, now you need to confirm whether IP route is reachable between Device1 and Device3.

- Device1 failed to log into Device3 using telnet IPv6 address, now you need to confirm whether IPv6 route is reachable between Device1 and Device3.

## Network Topology

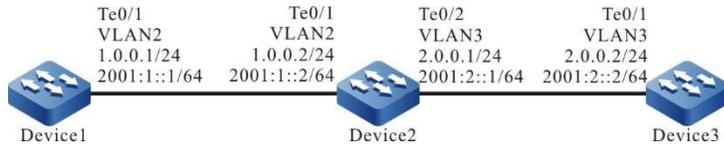


Figure 111-1 Network Topology for the Application of Ping

## Configuration Steps

Step 1: Configure the IP address and IPv6 global unicast address of each interface. (Omitted)

Step 2: Use the ping command to see if Device1 and Device3 are reachable to each other.

#Check whether Device1 ping Device3's IP address 2.0.0.2 can be pinged through.

```
Device1#ping 2.0.0.2

Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 2.0.0.2 , timeout is 2 seconds:
.....
Success rate is 0% (0/5).
```

#Check whether Device1 ping Device3's IPv6 address 2001:2::2 can be pinged through.

```
Device1#ping 2001:2::2

Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 2001:2::2 , timeout is 2 seconds:
.....
Success rate is 0% (0/5).
```

Step 3: Use the ping command to see if Device1 and Device2 are reachable to each other.

#Check whether Device1 ping Device2's IP address 1.0.0.2 can be pinged through.

```
Device1#ping 1.0.0.2

Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 1.0.0.2 , timeout is 2 seconds:
!!!!!!
Success rate is 100% (5/5). Round-trip min/avg/max = 0/0/0 ms.
```

#Check whether Device1 ping Device2's IPv6 address 2001:1::2 can be pinged through.

```
Device1#ping 2001:1::2

Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 2001:1::2 , timeout is 2 seconds:
!!!!!!
Success rate is 100% (5/5). Round-trip min/avg/max = 0/0/0 ms.
```

Step 4: Use the ping command to see if Device2 and Device3 are reachable to each other.

#Check whether Device2 ping Device3's IP address 2.0.0.2 can be pinged through.

```
Device2#ping 2.0.0.2
```

```
Press key (ctrl + shift + 6) interrupt it.  
Sending 5, 76-byte ICMP Echos to 2.0.0.2 , timeout is 2 seconds:  
!!!!  
Success rate is 100% (5/5). Round-trip min/avg/max = 0/0/0 ms.
```

#Check whether Device2 ping Device3's IPv6 address 2001:2::2 can be pinged through.

```
Device2#ping 2001:2::2
```

```
Press key (ctrl + shift + 6) interrupt it.  
Sending 5, 76-byte ICMP Echos to 2001:2::2 , timeout is 2 seconds:  
!!!!  
Success rate is 100% (5/5). Round-trip min/avg/max = 0/176/883 ms.
```

From the above troubleshooting results, we can see that Device1 can communicate with Device2, and Device2 can communicate with Device3. The problem appears between Device1 and Device3. You can view the routing and other configurations subsequently, or use the **debug ip icmp** command and **debug ipv6 icmp** command to check whether the contents of ICMP packets and ICMPv6 packets are correct respectively, or you can use the traceroute command introduced in the following section to confirm the faulty network node.

### 111.3.2 Application of Traceroute

#### Network Requirements

- Device1 failed to log in to Device3 using telnet IP address, now you need to confirm whether the IP route between Device1 and Device3 is reachable, if the route is not reachable, then you need to identify the faulty network node.
- Device1 failed to log in to Device3 using telnet IPv6 address, now you need to confirm whether the IPv6 route between Device1 and Device3 is reachable, if the route is not reachable, then you need to identify the faulty network node.

#### Network Topology

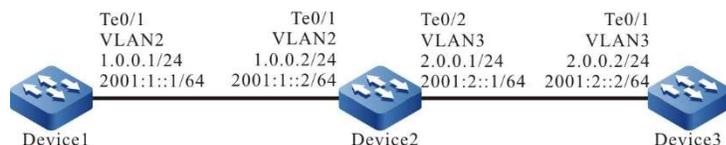


Figure 111-2 Network Topology for the Application of Traceroute

#### Configuration Steps

Step 1: Configure the IP address and IPv6 global unicast address of each interface. (Omitted)

Step 2: Use the traceroute command to identify the faulty node between Device1 and Device3.

#Use the traceroute command to identify the IPv4 faulty node between Device1 and Device3.

```
Device1#traceroute 2.0.0.2
Type escape sequence to abort.
Tracing the route to 2.0.0.2 , min ttl = 1, max ttl = 30 .

 1 1.0.0.2  0 ms  0 ms  0 ms
 2 * * *
 3 * * *
 4 * * *
 5 * * *
 6
```

Use the traceroute command to identify the IPv6 faulty node between Device1 and Device3.

```
Device1#traceroute 2001:2::2
Type escape sequence to abort.
Tracing the route to 2001:2::2 , min ttl = 1, max ttl = 30 .

 1 2001:1::2 0 ms  0 ms  0 ms
 2 * * *
 3 * * *
 4 * * *
 5 * * *
 6
```

From the above troubleshooting results, the traceroute packet from Device1 can reach Device2, and the traceroute packet from Device2 cannot reach Device3. Subsequently, you need to check the route configuration and lines of Device2 and Device3, or use the **debug ip icmp** command and **debug ipv6 icmp** command to check whether the content of ICMP packet and ICMPv6 packet is correct, and you can use the ping command in the previous section to check the connectivity between Device2 and Device3.

# 112 Keepalive Gateway

---

## 112.1 Overview

Keepalive gateway sets the Ethernet interface to send the keepalive packet to the specified gateway address, used to monitor the reachability of the destination gateway. When the gateway is unreachable, close the interface IP protocol layer.

After configuring the keepalive gateway on one interface, the interface regularly sends the ARP request packet to the configured gateway address. When the interface does not receive the ARP response packet for successive N times (N is the retry times configured for the user), close the interface IP protocol layer. Until receiving the ARP response packet again, enable the interface IP protocol layer.

## 112.2 Keepalive Gateway Function Configuration

Table 112-1 Keepalive Gateway Function Configuration List

Configuration Task	
Configure keepalive gateway.	Configure keepalive gateway basic functions.
	Configure the parameters for sending keepalive packets.
	Configure keepalive IPv6 associated gateway.

### 112.2.1 Configure Keepalive Gateway.

#### Configuration Condition

Before configuring the keepalive gateway function, do the following:

- Configure interface IP address.

### Configure Keepalive Gateway Basic Functions.

Table 112-2 Configuring Keepalive Gateway Basic Functions

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Configure keepalive gateway function.	<b>keepalive gateway</b> <i>ip-address</i> [high-prio] [ <i>interval</i>   <b>msec</b> <i>interval</i> ] [ <i>retry-count</i> ]	Mandatory  By default, the keepalive gateway function is not enabled on the interface.

### Configure the Parameters for Sending Keepalive Packets.

Configure the parameters for sending keepalive packets to control the sending rate of the keepalive gateway packets. When the sending rate of keepalive packets reaches the configured value, you can continue to send keepalive packets after the configured time is paused.

Table 112-3 Configuring Parameters for Sending Keepalive Packet

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the sending rate of keepalive packets.	<b>keepalive gateway disperse pkt-rate</b> <i>packet-rate</i>	Optional  By default, the maximum sending rate of keepalive packets is 100pps.
Configure the time for sending keepalive packets.	<b>keepalive gateway disperse pause-time</b> <i>pause-time</i>	Optional  By default, the time for sending keepalive packets is 100 milliseconds.

### Configure Keepalive IPv6 Associated Gateway.

When keepalive IPv6 associated gateway is configured, the IPv6 protocol layer of the interface will be turned off at the same time when the gateway is unreachable.

Table 112-4 Configuring Keepalive IPv6 Associated Gateway

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the sending rate of keepalive packets.	<b>keepalive gateway ipv6-respond-ipv4</b>	Optional By default, keepalive the IPv6 associated gateway is disabled.

### 112.2.2 Keepalive Gateway Monitoring and Maintaining

Table 112-5 Keepalive Gateway Monitoring and Maintaining

Command	Description
<b>clear keepalive gateway statistics</b> [ <i>interface-name</i> ]	Clear the incoming and inbound and outbound statistics of keepalive gateway.
<b>show keepalive gateway</b> [ <i>interface-name</i> ]	View interfaces with keepalive gateway enabled, and their configurations.
<b>show keepalive gateway disperse</b>	View the configuration of the sending parameters of the keepalive packets.
<b>show keepalive gateway statistics</b> [ <i>interface-name</i> ]	View statistics on gateway activities.

## 112.3 Typical Configuration Example of Keepalive Gateway

### 112.3.1 Configure Keepalive Gateway Function.

#### Network Requirements

- As a connecting device, Device 4 transmits the data in a transparent way.
- Device1, Device2, and Device3 are running the OSPF protocol for routing interactions.
- Device3 is preferred for the data flow from Device1 to the 201.0.0.0/24 network segment.
- The line between Device1 and Device3 has the enabled keepalive gateway. When the line between Device1 and Device3 fails, the keepalive gateway function will quickly detect the failure and modify the state of the relevant interface to down, and OSPF will switch the route to Device2 for communication after it senses the state change of the interface.

### Network Topology

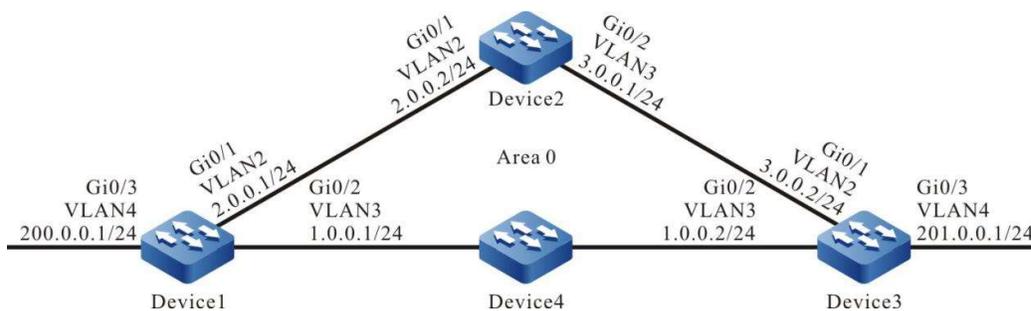


Figure 112-1 Network Topology for Configuring Keepalive Gateway

### Configuration Steps

- Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)
- Step 2: Configures IP addresses for the ports. (Omitted)
- Step 3: Configure OSPF process.

#### #Configure Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#network 1.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 200.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#exit
```

#### #Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#network 3.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#exit
```

#### #Configure Device3.

```
Device3#configure terminal
Device3(config)#router ospf 100
```

```
Device3(config-ospf)#network 1.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 3.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 201.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#exit
```

#### #View the routing table of Device1.

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, Ex - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C 1.0.0.0/24 is directly connected, 00:20:17, vlan3
C 2.0.0.0/24 is directly connected, 13:01:32, vlan2
O 3.0.0.0/24 [110/2] via 2.0.0.2, 01:11:40, vlan2
   [110/2] via 1.0.0.2, 00:02:00, vlan3
C 200.0.0.0/24 is directly connected, 01:31:58, vlan4
O 201.0.0.0/24 [110/2] via 1.0.0.2, 00:02:00, vlan3
```

#Device3 is preferred for the data flow from Device1 to the 201.0.0.0/24 network segment.

---

### Note

- Device2 and Device3 are viewed in the same way as Device1, and the viewing process is omitted.
- 

Step 4: Configure keepalive gateway.

#### #Configure Device1.

```
Device1(config)#interface vlan 3
Device1(config-if-vlan3)#keepalive gateway 1.0.0.2
Device1(config-if-vlan3)#exit
```

#### #Configure Device3.

```
Device3(config)#interface vlan 3
Device3(config-if-vlan3)#keepalive gateway 1.0.0.1
Device3(config-if-vlan3)#exit
```

#### #View the keepalive gateway information of Device1.

```
Device1#show keepalive gateway
interface vlan3 gateway 1.0.0.2 time 10s retry 3 remain 3 now UP
```

#### #View the keepalive gateway information of Device3.

```
Device3#show keepalive gateway
interface vlan3 gateway 1.0.0.1 time 10s retry 3 remain 3 now UP
```

Step 5: Check the result.

#When the line between Device1 and Device3 fails, the keepalive gateway function will quickly detect the failure and change the state of interface VLAN3 to down.

```
Device1#show keepalive gateway
interface vlan3 gateway 1.0.0.2 time 10s retry 3 remain 0 now DOWN
```

#OSPF senses the state change of interface VLAN3 and switches the route to Device2 for communication.

```
Device1# show ip ospf interface vlan3
VLAN3 is down, line protocol is down
  OSPF is enabled, but not running on this interface
```

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, Ex - IRMP external, o - SNSP, B - BGP, i-ISIS
```

```
Gateway of last resort is not set
```

```
C 2.0.0.0/24 is directly connected, 13:16:40, vlan2
O 3.0.0.0/24 [110/2] via 2.0.0.2, 00:01:25, vlan2
C 200.0.0.0/24 is directly connected, 00:10:53, vlan4
O 201.0.0.0/24 [110/3] via 2.0.0.2, 00:00:18, vlan2
```

# It is indicated that Device2 is preferred for the data flow from Device1 to the 201.0.0.1/24 network segment.

# 113 SLA

---

## 113.1 Overview

SLA (Service Level Agreements) calculates the related parameters according to the packet transmission and outputs the report at last. SLA, also called RTR (Response Time Reporter), is one network detection and monitoring tool. SLA regularly sends the packets of the specified protocol to detect and monitor the network communication. SLA can diagnose different network applications and output the test result by configuring different types of RTR entities and adjusting.

SLA basic concepts:

- RTR Entity: RTR Entity is one universal concept and not related with the specific type of RTR entity. The current RTR entity types of the system include: the ICMP-echo entity, ICMP-path-echo entity, ICMP-path-jitter entity, and UDP-echo entity used to detect the network communication; the VoIP-jitter entity used to detect the network transmitting the VoIP packets; the FLOW-statistics entity used to detect the interface traffic; the MAC-ping entity used to detect the Ethernet link communication service quality.
- RTR Group: One RTR entity group is the set of one or multiple entities;
- RTR responder: The RTR responder is configured at the destination, mainly used to set up the connection with the source and respond the detection packet sent by the source. Most entities do not need to configure the responder, but when using the UDP-echo entity and VoIP-jitter entity, we should configure the responder.
- RTR Schedule: If only configuring the RTR entity or RTR entity group, we cannot detect, but should initiate the scheduling so that the detection can be completed.

## 113.2 SLA Function Configuration

Table 113-1 SLA Function Configuration List

Configuration Task	
Enable RTR.	Enable RTR.

Configuration Task	
Configure an RTR entity.	Create an RTR entity.
	Configure ICMP-echo Entity
	Configure an ICMPv6-echo entity.
	Configure ICMP-path-echo Entity
	Configure ICMP-path-jitter Entity
	Configure VoIP-jitter Entity
	Configure UDP-echo Entity
	Configure FLOW-statistics Entity
	Configure entity common configuration.
Configure RTR Entity Group	Configure RTR Entity Group
Configure RTR Responder	Configure RTR Responder
Configure RTR Scheduler	Configure RTR Scheduler
Configure Pausing Scheduling Entity	Configure Pausing Scheduling Entity
Configure Restoring Scheduling Entity	Configure Restoring Scheduling Entity

### 113.2.1 Enable RTR.

Among the various configuration tasks of RTR, it must be enabled first before the configuration of other functional features can take effect.

#### Configuration Condition

None

#### Enable RTR.

Table 113-1 Enabling RTR

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable RTR.	<b>rtr enable</b>	Mandatory By default, RTR is not enabled.

### 113.2.2 Configure an RTR entity.

#### Configuration Condition

Before configuring an RTR entity, do the following:

Enable RTR.

#### Create an RTR entity.

There is one type of detection for each type of entity. After creating an RTR entity and entering the configuration mode for that entity, you can configure the specific parameters of the entity.

Table 113-3 Creating an RTR Entity

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Create an RTR entity.	<b>rtr <i>entity-id entity-type</i></b>	Mandatory

#### Configure ICMP-echo Entity

The ICMP-echo entity is to detect the network communication. It regularly sends the ICMP echo request packet to one destination address in the network, so as to get the delay and packet loss of the packet transmission from the detection end to the destination end. In one detection period, as long as the ICMP-echo entity receives one ICMP echo request response packet, the entity status is reachable.

The general network devices all support ping, so the entity can take effect in detecting the network communication. With the rich scheduling policies and log recording function, we can let the network administrator get to know the network communication status and history information in time and reduce inputting the common ping command frequently at the same time.

Table 113-4 Configuring an ICMP-Echo Entity

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the ICMP-echo entity configuration mode.	<b>rtr entity-id [ icmpecho ]</b>	-
Configure the detection attributes.	<b>set [ vrf vrf-name ] target-ip-address [ npacket ] [ data-size ] [ timeout ] [ frequency-value ] [ extend source-ip-address [ tos ] [ set-DF ] [ verify-data ] ]</b>	Mandatory  By default, no detection attribute of the entity is configured.
Configure to set the rtt value as the basis for determining whether the entity is reachable.	<b>status-care rtt</b>	Optional  By default, the rtt value is not used to determine whether the entity is reachable.
Configure entity common configuration.	Please refer to the section on configuring entity common configuration.	Optional

---

## Note

- The schedule interval (frequency-value) of the ICMP-echo entity needs to satisfy the following requirements: schedule interval > npacket \* timeout.
  - If a scheduler is configured for the entity, the aging time of the scheduler must be greater than the schedule interval for the entity.
- 

### Configuring ICMPv6-Echo Entities

The role of an ICMPV6-echo entity is to detect the network communication. It regularly sends the ICMP echo request packet to one destination address in the network, so as to get the delay and packet loss of the packet transmission from the detection end to the destination end. In one detection period, as long as the ICMPV6-echo entity receives one ICMP echo request response packet, the entity status is reachable.

The general network devices all support ping, so the entity can take effect in detecting the network communication. With the rich scheduling policies and log recording function, we can let the network administrator get to know the network communication status and history information in time and reduce inputting the common ping command frequently at the same time.

Table 113-5 Configuring an ICMPV6-Echo Entity

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the ICMP-echo entity configuration mode.	<b>rtr entity-id [ icmpv6echo ]</b>	-
Configure the detection attributes.	<b>set [ vrf vrf-name ] target-ip-address [ npacket ] [ data-size ] [ timeout ] [ frequency-value ] [ extend source-ip-address [ tos ] [ verify-data ] ]</b>	Mandatory By default, no detection attribute of the entity is configured.
Configure to set the rtt value as the basis for determining whether the entity is reachable.	<b>status-care rtt</b>	Optional By default, the rtt value is not used to determine whether the entity is reachable.
Configure entity common configuration.	Please refer to the section on configuring entity common configuration.	Optional

### Note

- The schedule interval (frequency-value) of the ICMPV6-echo entity needs to satisfy the following requirements: schedule interval > npacket \* timeout.
- If a scheduler is configured for the entity, the aging time of the scheduler must be greater than the schedule interval for the entity.

### Configure ICMP-path-echo Entity

The ICMP-path-echo entity is to detect the network communication. It regularly sends the ICMP echo request packet to one destination address in the network, so as to get the delay and packet loss of the packet transmission from the detection end to the destination end, as well as the delay and packet loss between the detection end and the intermediate devices from the detection end to the destination. In one detection period, as long as the ICMP-path-echo entity receives one ICMP echo request response packet, the entity status is reachable.

The general network devices all support ping, so the entity can take effect in detecting the network communication. With the rich scheduling policies and log recording function, we can let the network administrator get to know the network communication status (for example, which network device on the path has serious delay) and history information in time.

Table 113-6 Configuring an ICMP-Path-Echo Entity

Step	Command	Description
Enter the system configuration mode	<b>configure terminal</b>	-
Enter the ICMP-path-echo entity configuration mode.	<b>rtr <i>entity-id</i> [ icmp-path-echo ]</b>	-
Configure the detection attributes.	<b>set dest-ipaddr <i>target-ip-address</i></b> <b>[ source-ipaddr <i>source-ip-address</i> ]</b>	Mandatory
Configure loose source station routing.	<b>lsr-path [ <i>hop-ip-address-list</i>   none ]</b>	Optional By default, no loose source station routing is configured.
Configure to detect only the network conditions from the source to the destination.	<b>targetOnly [ true   false ]</b>	Optional By default, targetOnly is true to detect only the network conditions from the source to the destination.  If targetOnly is configured to false, it will detect the network conditions from the source to the destination hop by hop.

Step	Command	Description
Configure whether to verify the data content of the response packet.	<b>verify-data</b> [ true   false ]	Optional By default, no data content is verified.
Configure entity common configuration.	Please refer to the section on configuring entity common configuration.	Optional

### Configure ICMP-path-jitter Entity

The ICMP-path-jitter entity is to detect the network communication. It regularly sends the ICMP echo request packet to one destination address in the network, so as to get the delay, jitter, and packet loss of the packet transmission from the detection end to the destination end, as well as the delay, jitter and packet loss between the detection end and the intermediate devices from the detection end to the destination. In one detection period, as long as the ICMP-path-jitter entity receives one ICMP echo request response packet, the entity status is reachable.

The general network devices all support ping, so the entity can take effect in detecting the network communication. With the rich scheduling policies and log recording function, we can let the network administrator get to know the network communication status (for example, which network device on the path has serious delay) and history information in time.

Table 113-7 Configuring an ICMP-Path-Jitter Entity

Step	Command	Description
Enter the system configuration mode	<b>configure terminal</b>	-
Enter the ICMP-path-jitter entity configuration mode.	<b>rtr entity-id</b> [ icmp-path-jitter ]	-
Configure the detection attributes.	<b>set dest-ipaddr</b> <i>target-ip-address</i> [ <i>pkt-number</i> ] [ <i>pkt-interval</i> ] <b>[ source-ipaddr</b> <i>source-ip-address</i> ]	Mandatory
Configure the IP address of the loose source station routing.	<b>lsr-path</b> [ <i>hop-ip-address-list</i>   <b>none</b> ]	Optional By default, no source station routing is configured.

Step	Command	Description
Configure to detect only the network conditions from the source to the destination.	<b>targetOnly</b> [ true   false ]	Optional  By default, targetOnly is true to detect only the network conditions from the source to the destination.  If targetOnly is configured to false, it will detect the network conditions from the source to the destination hop by hop.
Configure the jitter threshold and the overrun rule.	<b>threshold-jitter</b> <i>jitter</i> <b>direction</b> { be   se }	Optional  By default, the jitter threshold is 6000 milliseconds and the overrun rule is be.
Configure whether to verify the data content of the response packet.	<b>verify-data</b> [ true   false ]	Optional  By default, no data content is verified.
Configure entity common configuration.	Please refer to the section on configuring entity common configuration.	Optional

---

## Note

- When the over-limit rule is be and the actual value is larger than or equal to the threshold, it is judged as over-limit; when the over-limit rule is se and the actual value is smaller than or equal to the threshold, it is judged as over-limit.
- 

### Configure VoIP-jitter Entity

The VoIP-jitter entity is the RTR entity used to measure the transmission quality of the VoIP packet in the general IP network.

The VoIP-jitter entity can simulate the G.711 A Law, G.711 mu Law, and G.729A codec or the customized codes to send the UDP packet with the corresponding rate, packet interval and size from the source device

to the destination device, measure the turnaround time, uni-directional packet loss and uni-directional delay of the packet, and calculates the ICPIF value based on the statistics information. At last, estimate the MOS value according to the ICPIF value. In the detection period, as long as the VoIP-jitter entity receives one detection response packet, the status of the entity is reachable.

Table 113-8 Configuring a VoIP-litter Entity

Step	Command	Description
Enter the system configuration mode	<b>configure terminal</b>	-
Enter the VoIP-jitter entity configuration mode.	<b>rtr <i>entity-id</i> [ jitter ]</b>	Mandatory If the entity already exists, go directly to entity configuration mode.
Configure the detection attributes.	<b>set dest-ipaddr <i>target-ip-address</i> dest-port <i>target-port</i> { g711alaw   g711ulaw   g729a   user_defined packet-size <i>packet-number</i> packet-interval <i>schedule-interval</i> } [ source-ipaddr <i>source-ip-address</i> ] [ source-port <i>source-port</i> ]</b>	Mandatory
Configure the source-to-destination one-way delay threshold and the overrun rule.	<b>threshold-sd-delay <i>sd-delay</i> direction { be   se }</b>	Optional By default, the source-to-destination delay threshold is 5000 milliseconds and the overrun rule is be.
Configure the source-to-destination one-way jitter threshold and the overrun rule.	<b>threshold-sd-jitter <i>sd-jitter</i> direction { be   se }</b>	Optional By default, the source-to-destination one-way jitter threshold is 6000 milliseconds, and the overrun rule is be.
Configure the source-to-destination packet loss threshold and the overrun rule.	<b>threshold-sd-pktloss <i>sd-packet</i> direction { be   se }</b>	Optional By default, the source-to-destination packet loss threshold is 60000, and the overrun rule is be.

Step	Command	Description
Configure the destination-to-source one-way delay threshold and the overrun rule.	<b>threshold-ds-delay</b> <i>ds-delay</i> <b>direction</b> { <b>be</b>   <b>se</b> }	Optional  By default, the destination-to-source delay threshold is 5000 milliseconds and the overrun rule is be.
Configure the destination-to-source one-way jitter threshold and the overrun rule.	<b>threshold-ds-jitter</b> <i>ds-jitter</i> <b>direction</b> { <b>be</b>   <b>se</b> }	Optional  By default, the destination-to-source one-way jitter threshold is 6000 milliseconds, and the overrun rule is be.
Configure the destination-to-source packet loss threshold and the overrun rule.	<b>threshold-ds-pktloss</b> <i>ds-packet</i> <b>direction</b> { <b>be</b>   <b>se</b> }	Optional  By default, the destination-to-source packet loss threshold is 60000, and the overrun rule is be.
Configure the threshold and the overrun rule for icpif value.	<b>threshold-icpif</b> <i>icpif-value</i> <b>direction</b> { <b>be</b>   <b>se</b> }	Optional  By default, the icpif threshold is 100000000, and the overrun rule is be.
Configure the threshold and the overrun rule for mos value.	<b>threshold-mos</b> <i>mos-value</i> <b>direction</b> { <b>be</b>   <b>se</b> }	Optional  By default, the mos threshold value is 10000000 and the overrun rule is be.
Configure entity common configuration.	Please refer to the section on configuring entity common configuration.	Optional

---

## Note

- When using the VoIP-jitter entity detection, besides configuring the VoIP-jitter entity, we also need to configure the RTR responder at the destination.
- By default, the VoIP-jitter entity sends many packets, which occupy the network

---

bandwidth, so when configuring the entity exceeds one hour, the shell prompts.

- When the VoIP-jitter entity detects the network transmitting the VoIP packet, the clocks of the source and the destination need to be consistent, so before scheduling the VoIP-jitter entity, we also need to configure the NTP server at the destination and NTP client at the source. After the clocks are synchronized, configure the RTR responder, and at last, configure the scheduler. For detailed configuration of NTP, please refer to NTP related sections in the User Manual.
  - When the over-limit rule is be and the actual value is larger than or equal to the threshold, it judged as over-limit; when the over-limit rule is se and the actual value is smaller than or equal to the threshold, it is judged as over-limit.
- 

### Configure UDP-echo Entity

The UDP-echo entity mainly detects the UDP packet transmitted in the IP network. In the entity, we need to specify the destination address and port of the sent packet. We can monitor the transmission of the UDP packet in the IP network by scheduling the entity. In one detection period, as long as the UDP-echo entity receives one detection response packet, the entity status is reachable.

The UDP-echo entity can monitor efficiently to record the turnaround delay, packet loss and other information of the UDP packet in the IP network, even record the monitored history information by logs so that the network administrator can get to know the network communication and fix the fault.

Table 113-9 Configuring an UDP-Echo Entity

Step	Command	Description
Enter the system configuration mode	<b>configure terminal</b>	-
Enter the UDP-echo entity configuration mode.	<b>rtr <i>entity-id</i> [ udpecho ]</b>	Mandatory If the entity already exists, go directly to entity configuration mode.
Configure the detection attributes.	<b>set dest-ipaddr <i>target-ip-address</i> dest-port <i>target-port</i> [ source-ipaddr <i>source-ip-address</i> ] [ source-port <i>source-port</i> ]</b>	Mandatory By default, the detection attribute of an UDP-echo entity is not configured.
Configure packet padding content.	<b>data-pattern <i>pad</i></b>	Optional By default, the padding content is "ABCD".

Step	Command	Description
Configure entity common configuration.	Please refer to the section on configuring entity common configuration.	Optional

## Note

- When using the UDP-echo entity detection, besides configuring the UDP-echo entity, we also need to configure the RTR responder at the destination.

### Configure FLOW-statistics Entity

The FLOW-statistics entity is to detect the interface traffic and one entity corresponds to one interface. We can monitor the traffic on the interface by scheduling the entity. In one detection period, as long as there are packets passing the interface monitored by the FLOW-statistics entity, the entity status is reachable.

The interval of the FLOW-statistics entity monitoring the interface traffic is 10s-10min. We can record the traffic peak value information on the interface by monitoring, even can record the history information of the traffic statistics during each monitoring, so as to make the network administrator get to know the network communication status and fix the fault.

Table 113-10 Configuring a FLOW-Statistics Entity

Step	Command	Description
Enter the system configuration mode	<b>configure terminal</b>	-
Enter the FLOW-statistics entity configuration mode.	<b>rtr entity-id [ flow-statistics ]</b>	Mandatory If the entity already exists, go directly to entity configuration mode.
Configure the detection attributes.	<b>flow-statistics interface</b> <i>interface-name interval interval</i>	Mandatory
Configure the inflow threshold and the	<b>threshold-inflow flow-value</b> <b>direction { be   se }</b>	Optional

Step	Command	Description
overrun rule for the interface.		By default, the inflow threshold of the interface is 200000000bps (bits/sec), and the overrun rule is be.
Configure the threshold for the number of packets received by the interface and the overrun rule.	<b>threshold-inpacket</b> <i>packet-value</i> <b>direction { be   se }</b>	Optional  By default, the threshold for the number of packets received by the interface is 200000000, and the overrun rule is be.
Configure the outflow threshold and the overrun rule for the interface.	<b>threshold-outflow</b> <i>flow-value</i> <b>direction { be   se }</b>	Optional  By default, the interface outflow threshold is 200000000 bps (bits per second), and the overrun rule is be.
Configure the threshold for the number of packets sent by the interface and the overrun rule.	<b>threshold-outpacket</b> <i>packet-value</i> <b>direction { be   se }</b>	Optional  By default, the threshold for the number of packets sent by the interface is 200000000, and the overrun rule is be.
Configure entity common configuration.	Please refer to the section on configuring entity common configuration.	Optional

---

## Note

- When the over-limit rule is be and the actual value is larger than or equal to the threshold, it is judged as over-limit; when the over-limit rule is se and the actual value is smaller than or equal to the threshold, it is judged as over-limit.
- 

### Configure Entity Common Configuration.

Table 113-11 Configuring Entity Common Configuration

Step	Command	Description
Configure alarm types.	<b>alarm-type</b> [ <b>log</b>   <b>log-and-trap</b>   <b>trap</b>   <b>none</b> ]	Optional By default, the alarm mode is none, i.e. no alarm.
Configure the number of history records to be saved.	<b>number-of-history-kept</b> <i>history-number</i>	Optional By default, 1 history record is saved.
Configure the period for saving history.	<b>periods</b> <i>periods</i>	Optional By default, 1 history record is saved at the end of each schedule.
Configure timeout.	<b>timeout</b> <i>timeout</i>	Optional By default, the timeout is: For ICMP-path-echo entity, the timeout is 5000 milliseconds. For ICMP-path-jitter entity, the timeout is 5000 milliseconds. For VoIP-jitter entity, the timeout is 50000 milliseconds. For UDP-echo entity, the timeout is 5000 milliseconds. Entities that do not support the common command: ICMP-echo entity ICMPv6-echo entity FLOW-statistics entity
Configure the TOS value of a packet.	<b>tos</b> <i>tos-value</i>	Optional By default, the TOS value is 0. Entities that do not support the common command: ICMP-echo entity ICMPv6-echo entity

Step	Command	Description
		FLOW-statistics entity
Configure the VRF attribute of an entity.	<b>vrf</b> <i>vrf-name</i>	Optional By default, the VRF attribute of entity is not configured. Entities that do not support the common command: ICMP-echo entity ICMPv6-echo entity FLOW-statistics entity
Configure the schedule interval for the entity.	<b>frequency</b> <i>seconds</i>	Optional By default, the schedule interval is: For ICMP-path-echo entity, the interval is 60 seconds. For ICMP-path-jitter entity, the interval is 60 seconds. For UDP-echo entity, the interval is 60 seconds. Entities that do not support the common command: ICMP-echo entity ICMPv6-echo entity VoIP-jitter entity FLOW-statistics entity
Configure the length of the detection packet.	<b>request-data-size</b> <i>data-size</i>	Optional By default, the length of a detection packet is: For ICMP-path-echo entity, the length is 70 bytes. For ICMP-path-jitter entity, the length is 70 bytes. For UDP-echo entity, the length is 16 bytes.

Step	Command	Description
		<p>Entities that do not support the common command:</p> <p>ICMP-echo entity</p> <p>ICMPv6-echo entity</p> <p>VoIP-jitter entity</p> <p>FLOW-statistics entity</p>
<p>Configure the packet loss threshold and the overrun rule.</p>	<p><b>threshold-pktloss</b> <i>pktloss</i> <b>direction</b> { <b>be</b>   <b>se</b> }</p>	<p>Optional</p> <p>By default, the packet loss threshold is:</p> <p>For ICMP-echo entity, the threshold is 150.</p> <p>For ICMPv6-echo entity, the threshold is 150.</p> <p>For ICMP-path-echo entity, the threshold is 1.</p> <p>For ICMP-path-jitter entity, the threshold is 100.</p> <p>For UDP-echo entity, the threshold is 1.</p> <p>The overrun rule is be.</p> <p>Entities that do not support the common command:</p> <p>VoIP-jitter entity</p> <p>FLOW-statistics entity</p>
<p>Configure the bi-directional delay threshold and the overrun rule.</p>	<p><b>threshold-rtt</b> <i>rtt</i> <b>direction</b> { <b>be</b>   <b>se</b> }</p>	<p>Optional</p> <p>By default, the bi-directional delay threshold is:</p> <p>For ICMP-echo entity, the threshold is 9000 milliseconds.</p> <p>For ICMPv6-echo entity, the threshold is 9000 milliseconds.</p> <p>For ICMP-path-echo entity, the threshold is 9000 milliseconds.</p>

Step	Command	Description
		<p>For ICMP-path-jitter entity, the threshold is 9000 milliseconds.</p> <p>For VoIP-jitter entity, the threshold is 9000 milliseconds.</p> <p>For UDP-echo entity, the threshold is 9000 milliseconds.</p> <p>The overrun rule is be.</p> <p>Entities that do not support the common command:</p> <p>FLOW-statistics entity</p>

---

## Note

- If the RTR entity already exists and the entity is in the un-scheduled state, execute the `rtr entity-id` command to enter the entity configuration mode directly.
  - When the over-limit rule is `be` and the actual value is larger than or equal to the threshold, it is judged as over-limit; when the over-limit rule is `se` and the actual value is smaller than or equal to the threshold, it is judged as over-limit.
  - The schedule interval of the ICMP-path-echo entity needs to meet the following requirement: `schedule interval > timeout`.
  - The schedule interval of the ICMP-path-jitter entity needs to meet the following requirements: `schedule interval > timeout`; `timeout` needs to meet the following requirements: `timeout > pkt-number * pkt-interval`; For the `pkt-number` parameter and the `pkt-interval` parameter, refer to the `set` command of the ICMP-path-echo entity.
  - When the schedule interval of the VoIP-jitter entity selects simulating G.711ALaw, G.711muLaw, and G.729A codec, it is necessary to meet the following requirement: `schedule interval > timeout + 5`; when selecting the customized codec, it is necessary to meet the following requirement: `schedule interval > schedule-interval + 5`; `schedule-interval` needs to meet the following requirement: `schedule-interval > packet-number * packet-interval`; for the `schedule-interval`, `packet-number` and `packet-interval` parameters, refer to the `set` command of the VoIP-jitter entity.
  - The schedule interval of the UDP-echo entity needs to meet the following requirement: `schedule interval > timeout + 5`.
- 

### 113.2.3 Configure RTR Entity Group

One RTR entity group is the set of one or multiple RTR entity groups. One RTR entity can belong to multiple RTR entity groups and the group cannot become the member of the group. One group can only contain one

member once. The RTR entity group is identified by the group ID uniquely and the group name is automatically generated by the system.

The RTR entity group is mainly to schedule one RTR set. The scheduling for the RTR entity group is equivalent to the scheduling for all RTR entities in the RTR entity group. The detection result is saved in the history records of the RTR entity.

### Configuration Condition

Before configuring an RTR entity group, do the following:

Enable RTR.

### Configure RTR Entity Group

Table 113-12 Configuring an RTR Entity Group

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the configuration mode of an RTR entity group.	<b>rtr group</b> <i>group-id</i>	Mandatory If no corresponding RTR entity group exist, it will be created automatically.
Add members to an RTR entity group.	<b>member</b> <i>entity-list</i>	Optional By default, an RTR entity group does not contain any members.
Configure options of an RTR entity group.	<b>option {or   and }</b>	Optional By default, the status option of an RTR entity group is and (the group status is showed as reachable when all entities in the group are reachable).
Configure the schedule interval between members within the RTR entity group.	<b>interval</b> <i>interval</i>	Optional By default, the schedule interval for group members is 0 seconds.

Step	Command	Description
Configure the RTR entity group to automatically generate a scheduler.	<b>group probe</b>	Optional By default, the RTR entity group is not configured to auto-generate a scheduler.

## Note

- One VoIP-jitter entity or UDP-echo entity cannot be added to multiple groups for scheduling. Otherwise, the scheduling result may be wrong.
- The calculation method for the scheduling interval of the RTR entity group is as follows: scheduling interval = the maximum of all member scheduling intervals + (member quantity – 1) \* scheduling interval between the members.

### 113.2.4 Configure RTR Responder

The RTR responder is mainly used to set up the connection with the source end and respond the detection packets sent by the source end, so as to ensure that the detection result is correct. The VoIP-jitter entity and the UDP-echo entity need to set up the connection with the destination end, so we should configure the RTR responder at the destination end.

#### Configuration Condition

Before configuring an RTR entity responder, do the following:

Enable RTR.

#### Configure RTR Responder

Table 113-13 Configuring an RTR Responder

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure RTR Responder	<b>rtr responder</b>	Mandatory By default, no RTR responder is configured.

### 113.2.5 Configure RTR Scheduler

The RTR scheduler is the policy of the scheduling detection for the RTR entity or group. The RTR scheduler can take one entity member as the object and also can take one RTR entity group as the object, but cannot take the group and entity as the object together. The RTR scheduler is identified by the schedule ID uniquely and not related with the RTR entity type, but the scheduling interval should consider the attributes of the scheduled RTR entity or the members in the RTR entity group. The RTR scheduler provides rich scheduling policies and can select to schedule at once or start to schedule after some time, even can set the absolute time of starting the scheduling. Besides, the scheduler can automatically demise after the set scheduling times and also can always exist.

#### Configuration Condition

Before configuring an RTR scheduler, do the following:

Configure the RTR entity or RTR entity group that need to be scheduled.

#### Configure RTR Scheduler

Table 113-14 Configuring an RTR Scheduler

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure an RTR scheduler to schedule an entity or group.	<b>rtr schedule</b> <i>schedule-id</i> { <b>entity</b> <i>entity-id</i>   <b>group</b> <i>group-id</i> } <b>start</b> { <i>hh:mm</i> [ <i>:ss</i> ]   <i>date month year</i>   <b>after</b> <i>hh:mm</i> [ <i>:ss</i> ]   <b>now</b> } <b>ageout</b> <i>ageout-time</i> <b>life</b> { <b>forever</b>   <i>life-time</i> } <b>repeat</b> <i>repeat-times</i> }	Mandatory  By default, no RTR scheduler is configured.

---

#### Note

- The age time of the RTR scheduler should be larger than the scheduling interval of the scheduling object. Otherwise, after one scheduling, the scheduler is deleted because of aging and timeout.
- 

### 113.2.6 Configure Pausing Scheduling Entity

For an entity undergoing scheduling, you can configure to suspend schedule of that entity.

### Configuration Condition

Before configuring to suspend entity schedule, do the following:

The entity is in scheduling.

### Configure Pausing Scheduling Entity

Table 113-15 Configuring to Suspend Entity Schedule

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure Pausing Scheduling Entity	<b>rtr <i>entity-id</i> halt</b>	Optional By default, an entity in schedule is not suspended.

---

### Note

- Only one entity can configure rtr halt. If the entity is the member of the RTR entity group, we cannot configure rtr halt.
  - After configuring rtr halt and if still not configuring rtr resume before the scheduling period ends, the scheduler of scheduling the entity is deleted because of aging and timeout.
- 

### 113.2.7 Configure Restoring Scheduling Entity

For entities that are suspended from scheduling, you can configure to resume scheduling of that entity.

### Configuration Condition

Before configuring to recover schedule of an entity, do the following:

- The entity is suspended from scheduling.

### Configure Pausing Scheduling Entity

Table 113-16 Configuring Pausing Entity Scheduling

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure Restoring Scheduling Entity	<b>rtr <i>entity-id</i> resume</b>	Optional

## 113.2.8 SLA Monitoring and Maintaining

Table 113-17 SLA Monitoring and Maintaining

Command	Description
<b>show rtr entity</b> [ <i>entity-id</i> ]	Display information about an RTR entity.
<b>show rtr group</b> [ <i>group-id</i> ]	Display information about an RTR entity group.
<b>show rtr history</b> <i>entity-id</i>	Display history records of a specified RTR entity.
<b>show rtr schedule</b> [ <i>schedule-id</i> ]	Display information about an RTR scheduler.

## 113.3 Typical Configuration Example of SLA

### 113.3.1 Configure an ICMP-echo Entity to Detect the Network Communication

#### Network Requirements

- The ICMP-echo entity is used on Device1 to detect the network communication from Device1 to Device3.

#### Network Topology

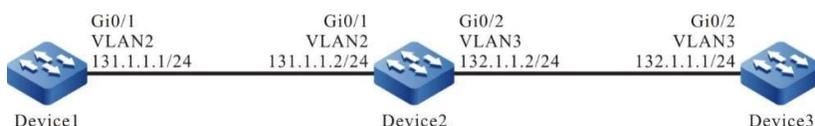


Figure 113-1 Network Topology for Configuring an ICMP-Echo Entity

#### Configuration Steps

- Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)
- Step 2: Configure the IP address and route of each interface to enable communication between Device1 and Device3. (Omitted)
- Step 3: Configure an ICMP-echo-type entity and add attribute parameters.

#Configure Device1.

```
Device1#config terminal
Device1(config)#rtr enable
Device1(config)#rtr 1 icmpEcho
Device1(config-rtr-icmpEcho)#set 132.1.1.1 5 70 2 12 extend 131.1.1.1 0 TRUE FALSE
Device1(config-rtr-icmpEcho)#alarm-type log
Device1(config-rtr-icmpEcho)#number-of-history-kept 255
Device1(config-rtr-icmpEcho)#threshold-pktLoss 10 direction be
Device1(config-rtr-icmpEcho)#threshold-rtt 1000 direction be
Device1(config-rtr-icmpEcho)#exit
```

#View the parameters of an ICMP-echo entity.

```
Device1#show rtr entity 1
-----
ID:1      name:IcmpEcho1      Created:TRUE
*****type:ICMPECHO*****
CreatedTime:WED OCT 31 14:49:31 2012
LatestModifiedTime:WED OCT 31 14:53:53 2012
Times-of-schedule:0
TargetIp:132.1.1.1
Transmit-packets:5
Totally-send-packets:0
Packet-size:70
Timeout:2(s)
Alarm-type:log
Threshold-of-rtt:1000(ms) direction:be
Threshold-of-packet-loss:10 direction:be
Number-of-history-kept:255
Periods:1
Extend parameters:
sourceIp:131.1.1.1  tos:0  DF(DON'T FRAG):TRUE  Verify-data:FALSE
In-scheduling:FALSE
Schedule frequency:12(s)
Status:DEFAULT
```

The results show that the entity parameters are consistent with the configuration.

In-scheduling:FALSE indicates that the entity is not scheduled.

Status:DEFAULT indicates that the entity status is DEFAULT.

---

 **Note**

- When an entity is not scheduled, its status is DEFAULT; when an entity is scheduled, if the entity is reachable, its status is REACHABLE, if it is unreachable, its status is UNREACHABLE.
-

Step 4: Schedule a defined ICMP-echo entity, and define attribute parameters of the schedule.

#### #Configure Device1

```
Device1(config)#rtr schedule 1 entity 1 start now ageout 100 life forever
```

Step 5: Check the result.

1) When the network communication from Device1 to Device3 is normal.

#### #View the status of an entity.

```
Device1#show rtr entity 1
-----
ID:1      name:IcmpEcho1    Created:TRUE
*****type:ICMPECHO*****
CreatedTime:WED OCT 31 14:49:31 2012
LatestModifiedTime:WED OCT 31 14:53:53 2012
Times-of-schedule:1
Time-of-last-schedule:WED OCT 31 14:54:07 2012
TargetIp:132.1.1.1
Transmit-packets:5
Totally-send-packets:5
Packet-size:70
Timeout:2(s)
Alarm-type:log
Threshold-of-rtt:1000(ms) direction:be
Threshold-of-packet-loss:10 direction:be
Number-of-history-kept:255
Periods:1
Extend parameters:
sourceIp:131.1.1.1  tos:0  DF(DONT FRAG):TRUE  Verify-data:FALSE
In-scheduling:TRUE
Schedule frequency:12(s)
Status:REACHABLE
```

In-scheduling:TRUE indicates that the entity is in scheduling.

Status: REACHABLE means that the entity status is reachable, that is, the network communication from Device1 to Device3 is normal.

1) When the network communication from Device1 to Device3 fails.

Since the entity parameters are configured with the alarm mode as log, the alarm message is printed on the device when the network is down, as follows:

```
Oct 31 14:54:46: [tRtrIcmpRev]Rtr 1 (ICMPECHO) rtt [9000ms] was exceeded(>=) threshold [1000ms].
```

#### #View the status of an entity.

```
Device1#show rtr entity 1
-----
ID:1      name:IcmpEcho1    Created:TRUE
*****type:ICMPECHO*****
CreatedTime:WED OCT 31 14:49:31 2012
LatestModifiedTime:WED OCT 31 14:53:53 2012
Times-of-schedule:4
Time-of-last-schedule:WED OCT 31 14:54:43 2012
TargetIp:132.1.1.1
Transmit-packets:5
```

```
Totally-send-packets:20
Packet-size:70
Timeout:2(s)
Alarm-type:log
Threshold-of-rtt:1000(ms) direction:be
Threshold-of-packet-loss:10 direction:be
Number-of-history-kept:255
Periods:1
Extend parameters:
sourceIp:131.1.1.1 tos:0 DF(DON'T FRAG):TRUE Verify-data:FALSE
In-scheduling:TRUE
Schedule frequency:12(s)
Status:UNREACHABLE
```

In-scheduling:TRUE indicates that the entity is in scheduling.

Status: UNREACHABLE means that the entity status is unreachable, that is, the network communication from Device1 to Device3 fails.

#View the history records.

```
Device1#show rtr history 1
-----
ID:1 Name:IcmpEcho1 CurHistorySize:4 MaxHistorysize:255
History recorded as following:
WED OCT 31 14:54:46 2012
  PktLoss:5 ,Rtt:invalid
WED OCT 31 14:54:32 2012
  PktLoss:0 ,Rtt:11 (ms)
WED OCT 31 14:54:20 2012
  PktLoss:0 ,Rtt:2 (ms)
WED OCT 31 14:54:07 2012
  PktLoss:0 ,Rtt:2 (ms)
```

The history records provide details about the packet loss and latency of each schedule; an invalid Rtt indicates that there is a failure in the network causing the network to be unreachable.

### 113.3.2 Configure an ICMP-path-echo Entity to Detect the Network Communication

#### Network Requirements

- An ICMP-path-echo entity is used on Device1 to detect the network communication of the path from Device1 to Device3.

#### Network Topology



Figure 113-1 Network Topology for Configuring an ICMP-Path-Echo Entity

#### Configuration Steps

Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configure the IP address and route of each interface to enable communication between Device1, Device2 and Device3. (Omitted)

Step 3: Configure an ICMP-path-echo-type entity and add attribute parameters.

#Configure Device1.

```
Device1#config terminal
Device1(config)#rtr enable
Device1(config)#rtr 1 icmp-path-echo
Device1(config-rtr-icmpppathecho)#set dest-ipaddr 192.0.0.2 source-ipaddr 110.1.0.1
Device1(config-rtr-icmpppathecho)#number-of-history-kept 255
Device1(config-rtr-icmpppathecho)#targetOnly false
Device1(config-rtr-icmpppathecho)#exit
```

#View the parameters of an ICMP-path-echo entity.

```
Device1#show rtr entity 1
-----
ID:1      name:IcmpPathEcho1      Created:TRUE
*****type:ICMPATHECHO*****
CreatedTime:WED OCT 24 10:18:02 2012
LatestModifiedTime:WED OCT 24 10:19:09 2012
Times-of-schedule:0
TargetIp:192.0.0.2
SourceIp:110.1.0.1
Transmit-packets:1 (each hop)
Request-data-size:70
Timeout:5000(ms)
Frequency:60(s)
TargetOnly:FALSE
Verify-data:FALSE
Alarm-type:none
Threshold-of-rtt:9000(ms) direction:be
Threshold-of-pktloss:1 direction:be
Number-of-history-kept:255
Periods:1
In-scheduling:FALSE
Status:DEFAULT
-----
```

The results show that the entity parameters are consistent with the configuration.

In-scheduling:FALSE indicates that the entity is not scheduled.

Status:DEFAULT indicates that the entity status is DEFAULT.

Step 4: Schedule a defined ICMP-path-echo entity, and define attribute parameters of the schedule.

#Configure Device1.

```
Device1(config)#rtr schedule 1 entity 1 start now ageout 100 life 600 repeat 10
```

Step 5: Check the result.

#View the status of an entity.

```
Device1#show rtr entity 1
```

```

-----
ID:1      name:IcmpPathEcho1      Created:TRUE
*****type:ICMPATHECHO*****
CreatedTime:WED OCT 24 10:18:02 2012
LatestModifiedTime:WED OCT 24 10:19:09 2012
Times-of-schedule:1
Time-of-last-schedule:WED OCT 24 10:20:01 2012
TargetIp:192.0.0.2
SourceIp:110.1.0.1
Transmit-packets:1 (each hop)
Request-data-size:70
Timeout:5000(ms)
Frequency:60(s)
TargetOnly:FALSE
Verify-data:FALSE
Alarm-type:none
Threshold-of-rtt:9000(ms) direction:be
Threshold-of-pktloss:1 direction:be
Number-of-history-kept:255
Periods:1
In-scheduling:TRUE
Status:REACHABLE

```

In-scheduling:TRUE indicates that the entity is in scheduling.

Status: REACHABLE means that the entity status is reachable, that is, the network communication of the path from Device1 to Device3 is normal.

#View the history records.

```

Device1#show rtr history 1
-----
ID:1 Name:IcmpPathEcho1
History of hop-by-hop:
110.1.0.2 PktLoss:0 ,Rtt:2 (ms)
192.0.0.2 PktLoss:0 ,Rtt:1 (ms)
History of record from source to dest:
CurHistorySize:1 MaxHistorysize:255
WED OCT 24 10:20:01 2012
PktLoss:0 ,Rtt:1 (ms)

```

The history records provide details about the packet loss and latency of each schedule.

#Wait for a while and view the entity status after 10 schedule sessions.

```

Device1#show rtr entity 1
-----
ID:1      name:IcmpPathEcho1      Created:TRUE
*****type:ICMPATHECHO*****
CreatedTime:WED OCT 24 10:18:02 2012
LatestModifiedTime:WED OCT 24 10:19:09 2012
Times-of-schedule:10
Time-of-last-schedule:WED OCT 24 10:29:01 2012
TargetIp:192.0.0.2
SourceIp:110.1.0.1
Transmit-packets:1 (each hop)
Request-data-size:70
Timeout:5000(ms)
Frequency:60(s)
TargetOnly:FALSE
Verify-data:FALSE
Alarm-type:none
Threshold-of-rtt:9000(ms) direction:be
Threshold-of-pktloss:1 direction:be
Number-of-history-kept:255
Periods:1
In-scheduling:FALSE
Status:DEFAULT

```

After 10 scheduling sessions, the scheduling stops and the entity status is DEFAULT.

### 113.3.3 Configure an ICMP-path-jitter Entity to Detect the Network Communication

#### Network Requirements

- An ICMP-path-jitter entity is used on Device1 to detect the network communication of the path from Device1 to Device3.

#### Network Topology



Figure 113-2 Network Topology for Configuring an ICMP-Path-Jitter Entity

#### Configuration Steps

- Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)
- Step 2: Configure the IP address and route of each interface to enable communication between Device1, Device2 and Device3. (Omitted)
- Step 3: Configure an ICMP-path-jitter-type entity and add attribute parameters.

#### #Configure Device1.

```
Device1#config terminal
Device1(config)#rtr enable
Device1(config)#rtr 1 icmp-path-jitter
Device1(config-rtr-icmppathjitter)#set dest-ipaddr 192.0.0.2 10 20 source-ipaddr 110.1.0.1
Device1(config-rtr-icmppathjitter)#number-of-history-kept 255
Device1(config-rtr-icmppathjitter)#targetOnly false
Device1(config-rtr-icmppathjitter)#exit
```

#### #View the parameters of an ICMP-path-jitter.

```
Device1#show rtr entity 1
-----
ID:1      name:IcmpPathJitter1      Created:TRUE
*****type:ICMPATHJITTER*****
CreatedTime:WED OCT 24 10:54:31 2012
LatestModifiedTime:WED OCT 24 10:56:12 2012
Times-of-schedule:0
TargetIp:192.0.0.2
SourceIp:110.1.0.1
Transmit-packets:10 (each hop)
Packets-interval:20(ms)
Request-data-size:70
Timeout:5000(ms)
Frequency:60(s)
TargetOnly:FALSE
Verify-data:FALSE
Alarm-type:none
Threshold-of-rtt:9000(ms) direction:be
```

```
Threshold-of-pktLoss: 200000000 direction:be
Threshold-of-jitter:6000(ms) direction:be
Number-of-history-kept:255
Periods:1
In-scheduling:FALSE
Status:DEFAULT
-----
```

The results show that the entity parameters are consistent with the configuration.

In-scheduling:FALSE indicates that the entity is not scheduled.

Status:DEFAULT indicates that the entity status is DEFAULT.

Step 4: Schedule a defined ICMP-path-jitter entity, and define attribute parameters of the schedule.

#Configure Device1.

```
Device1(config)#rtr schedule 1 entity 1 start now ageout 100 life forever
```

Step 5: Check the result.

#View the status of an entity.

```
Device1#show rtr entity 1
-----
ID:1      name:IcmpPathJitter1      Created:TRUE
*****type:ICMPATHJITTER*****
CreatedTime:WED OCT 24 10:54:31 2012
LatestModifiedTime:WED OCT 24 10:56:12 2012
Times-of-schedule:4
Time-of-last-schedule:WED OCT 24 11:00:25 2012
TargetIp:192.0.0.2
SourceIp:110.1.0.1
Transmit-packets:10 (each hop)
Packets-interval:20(ms)
Request-data-size:70
Timeout:5000(ms)
Frequency:60(s)
TargetOnly:FALSE
Verify-data:FALSE
Alarm-type:none
Threshold-of-rtt:9000(ms) direction:be
Threshold-of-pktLoss: 200000000 direction:be
Threshold-of-jitter:6000(ms) direction:be
Number-of-history-kept:255
Periods:1
In-scheduling:TRUE
Status:REACHABLE
-----
```

In-scheduling:TRUE indicates that the entity is in scheduling.

Status: REACHABLE means that the entity status is reachable, that is, the network communication from Device1 to Device2 is normal.

#View the history records.

```
Device1#show rtr history 1
-----
ID:1 Name:IcmpPathJitter1
History of hop-by-hop:
```

```

110.1.0.2 PktLoss:0 Rtt:1 (ms),Jitter:0 (ms)
192.0.0.2 PktLoss:0 Rtt:0 (ms),Jitter:0 (ms)
History of record from source to dest:
CurHistorySize:4 MaxHistorysize:255
WED OCT 24 11:00:25 2012
PktLoss:0 ,Rtt:1 (ms),Jitter:0 (ms)
WED OCT 24 10:59:25 2012
PktLoss:0 ,Rtt:0 (ms),Jitter:0 (ms)
WED OCT 24 10:58:25 2012
PktLoss:0 ,Rtt:0 (ms),Jitter:0 (ms)
WED OCT 24 10:57:25 2012
PktLoss:0 ,Rtt:0 (ms),Jitter:0 (ms)
-----

```

The history records provide details about the packet loss, latency and jitter of each schedule.

### 113.3.4 Configuring a VoIP-jitter Entity to Detect Network Transmission of Voice Packets

#### Network Requirements

- A VoIP-jitter entity is used on Device1 to detect the transmission of voice packets from Device1 to Device3.

#### Network Topology



Figure 113-113 Network Topology for Configuring VoIP-Jitter Entities

#### Configuration Steps

- Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)
- Step 2: Configure the IP address and route of each interface to enable communication between Device1 and Device3. (Omitted)
- Step 3: Configure ntp for clock synchronization.

#Configure Device3.

```

Device3#config terminal
Device3(config)#ntp master

```

#Configure Device1.

```

Device1(config)#ntp server 192.0.0.2

```

#View if Device3 has been successfully specified as the clock server, indicating that the clock has been synchronized.

```

Device3#show ntp status
Current NTP status information
Clock is synchronized, stratum 8, reference is 127.127.8.10

```

reference time is D4321EF4.7BBBBB68 (08:01:56.483 Wed Oct 24 2012)

#View if Device1 has been successfully specified as a clock client, indicating that the clock has been synchronized with the server address displayed.

```
Device1#show ntp status
Current NTP status information
Clock is synchronized, stratum 9, reference is 192.0.0.2
reference time is D43222C1.91110F31 (08:18:09.566 Wed Oct 24 2012)
```

Step 4: Configure a responder on Device3 as the responder.

#Configure Device3

```
Device3(config)#rtr enable
Device3(config)#rtr responder
```

Step 5: Configure the VoIP-jitter entity on Device1 and add the attribute parameters.

#Configure Device1.

```
Device1#config terminal
Device1(config)#rtr enable
Device1(config)#rtr 1 jitter
Device1(config-rtr-jitter)#set dest-ipaddr 192.0.0.2 dest-port 1234 g711alaw source-ipaddr 110.1.0.1 source-port 1234
Device1(config-rtr-jitter)#number-of-history-kept 255
Device1(config-rtr-jitter)#exit
```

#View the entity parameters.

```
Device1#show rtr entity 1
-----
ID:1      name:Jitter1      Created:TRUE
*****type:JITTER*****
CreatedTime:WED OCT 24 16:02:32 2012
LatestModifiedTime:WED OCT 24 16:02:58 2012
Times-of-schedule:0
Entry-state:Pend
TargetIp:192.0.0.2  targetPort:1234
Codec:G.711 A-Law  Packet-size:172 Packet-number:1000
Packet-transmit-interval:20(ms)
frequency:60(s)
SourceIp:110.1.0.1  Soure-port:1234
TimeOut:50000(ms)
Alarm-type:none
Threshold-of-dsDelay:5000(ms) direction:be
Threshold-of-dsJitter:6000(ms) direction:be
Threshold-of-dsPktLoss:200000000 direction:be
Threshold-of-sdDelay:5000(ms) direction:be
Threshold-of-sdJitter:6000(ms) direction:be
Threshold-of-sdPktLoss:200000000 direction:be
Threshold-of-rtt:9000(ms) direction:be
Threshold-of-mos:10000000 direction:be
Threshold-of-icipif:100000000 direction:be
Number-of-history-kept:255
Periods:1
Status:DEFAULT
-----
```

The results show that the entity parameters are consistent with the configuration.

Status:DEFAULT indicates that the entity status is DEFAULT.

Step 6: Invoke the defined VoIP-jitter entity and define attribute parameters of the schedule.

#Configure Device1.

```
Device1(config)#rtr schedule 1 entity 1 start now ageout 100 life 600 repeat 10
```

Step 7: Check the result.

#View the status of an entity.

```
Device1#show rtr entity 1
-----
ID:1      name:Jitter1      Created:TRUE
*****type:JITTER*****
CreatedTime:WED OCT 24 16:02:32 2012
LatestModifiedTime:WED OCT 24 16:06:02 2012
Times-of-schedule:3
Time-of-last-schedule:WED OCT 24 16:08:29 2012
Entry-state:Transmit
TargetIp:192.0.0.2  targetPort:1234
Codec:G.711 A-Law  Packet-size:172 Packet-number:1000
Packet-transmit-interval:20(ms)
frequency:60(s)
SourceIp:110.1.0.1  Soure-port:1234
TimeOut:50000(ms)
Alarm-type:none
Threshold-of-dsDelay:5000(ms) direction:be
Threshold-of-dsJitter:6000(ms) direction:be
Threshold-of-dsPktLoss:200000000 direction:be
Threshold-of-sdDelay:5000(ms) direction:be
Threshold-of-sdJitter:6000(ms) direction:be
Threshold-of-sdPktLoss:200000000 direction:be
Threshold-of-rtt:9000(ms) direction:be
Threshold-of-mos:10000000 direction:be
Threshold-of-icpif:100000000 direction:be
Number-of-history-kept:255
Periods:1
Status:REACHABLE
-----
```

Entry-state:Transmit indicates that the entity is in scheduling.

Status: REACHABLE means that the entity is reachable, indicating that the network from Device1 to Device3 is transmitting voice packets normally.

#View the history records.

```
Device1#show rtr history 1
-----
ID:1 Name:Jitter1 CurHistorySize:3 MaxHistorysize:255
History recorded as following:
WED OCT 24 16:08:46 2012
  SdPktLoss:0 ,DsPktLoss:0 ,Rtt:185 (ms),
  SdDelay:14 (ms),DsDelay:178 (ms),SdJitter:8 (ms),DsJitter:183 (ms),
  Mos:5.000000 ,icpif:0.000000
WED OCT 24 16:07:45 2012
  SdPktLoss:0 ,DsPktLoss:0 ,Rtt:14 (ms),
  SdDelay:16 (ms),DsDelay:7 (ms),SdJitter:10 (ms),DsJitter:13 (ms),
  Mos:5.000000 ,icpif:0.000000
WED OCT 24 16:06:46 2012
  SdPktLoss:0 ,DsPktLoss:0 ,Rtt:17 (ms),
  SdDelay:16 (ms),DsDelay:9 (ms),SdJitter:11 (ms),DsJitter:13 (ms),
  Mos:5.000000 ,icpif:0.000000
```

-----

The history records provide details about one-way packet loss, round-trip delay, one-way delay, and one-way jitter for each schedule.

---

## Note

- Before a VoIP-jitter entity is configured, the NTP service needs to be configured to achieve network clock synchronization and the rtr responder command needs to be configured on the destination end to set it as the responder. Note that the scheduling result will be incorrect if the clock is not synchronized or the responder is not configured.
- 

### 113.3.5 Configuring a UDP-echo Entity to Detect Network Transmission of UDP Packets

#### Network Requirements

- A UDP-echo entity is used on Device1 to detect the transmission of UDP packets from Device1 to Device3.

#### Network Topology



Figure 3-4 Network Topology for Configuring UDP-Echo Entities

#### Configuration Steps

- Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)
- Step 2: Configure the IP address and route of each interface to enable communication between Device1 and Device3. (Omitted)
- Step 3: Configure a responder on Device3 as the responder.

#### #Configure Device3

```
Device3#config terminal
Device3(config)#rtr enable
Device3(config)#rtr responder
```

- Step 4: Configure the UDP-echo entity on Device1 and add the attribute parameters.

#### #Configure Device1.

```

Device1#config terminal
Device1(config)#rtr enable
Device1(config)#rtr 1 udpecho
Device1(config-rtr-udpecho)#set dest-ipaddr 192.0.0.2 dest-port 1001 source-ipaddr 110.1.0.1 source-port 1001
Device1(config-rtr-udpecho)#number-of-history-kept 255
Device1(config-rtr-udpecho)#frequency 10
Device1(config-rtr-udpecho)#exit

```

**#View the entity parameters.**

```

Device1#show rtr entity 1
-----
ID:1      name:UdpEcho1      Created:TRUE
*****type:UDPECHO*****
CreatedTime:WED OCT 24 16:36:45 2012
LatestModifiedTime:WED OCT 24 16:37:44 2012
Times-of-schedule:0
Entry-state:Pend
TargetIp:192.0.0.2  TargetPort:1001
SourceIp:110.1.0.1  SourePort:1001
TimeOut:5000(ms)
request-data-size:16
Frequecy:10(s)
Alarm-type:none
Threshold-of-rtt:9000(ms) direction:be
Threshold-of-pktloss:1 direction:be
Number-of-history-kept:255
Periods:1
Status:DEFAULT
-----

```

The results show that the entity parameters are consistent with the configuration.

Status:DEFAULT indicates that the entity status is DEFAULT.

Step 5: Call the defined UDP-echo entity and define attribute parameters of the schedule.

**#Configure Device1.**

```

Device1(config)#rtr schedule 1 entity 1 start now ageout 100 life forever

```

Step 6: Check the result.

**#View the status of an entity.**

```

Device1#show rtr entity 1
-----
ID:1      name:UdpEcho1      Created:TRUE
*****type:UDPECHO*****
CreatedTime:WED OCT 24 16:36:45 2012
LatestModifiedTime:WED OCT 24 16:37:44 2012
Times-of-schedule:5
Time-of-last-schedule:WED OCT 24 16:39:50 2012
Entry-state:Pend
TargetIp:192.0.0.2  TargetPort:1001
SourceIp:110.1.0.1  SourePort:1001
TimeOut:5000(ms)
request-data-size:16
Frequecy:10(s)
Alarm-type:none
Threshold-of-rtt:9000(ms) direction:be
Threshold-of-pktloss:1 direction:be
Data-pattern:ABCD
Number-of-history-kept:255

```

```
Periods:1
Status:REACHABLE
```

Status: REACHABLE means that the entity is reachable, that is, the network from Device1 to Device3 is transmitting UDP packets normally.

#View the history records.

```
Device1#show rtr history 1
-----
ID:1 Name:UdpEcho1 CurHistorySize:5 MaxHistorysize:255
History recorded as following:
WED OCT 24 16:39:54 2012
    PktLoss:0 ,Rtt:1 (ms)
WED OCT 24 16:39:44 2012
    PktLoss:0 ,Rtt:1 (ms)
WED OCT 24 16:39:33 2012
    PktLoss:0 ,Rtt:2 (ms)
WED OCT 24 16:39:23 2012
    PktLoss:0 ,Rtt:2 (ms)
WED OCT 24 16:39:13 2012
    PktLoss:0 ,Rtt:2 (ms)
-----
```

The history records provide details about the packet loss and latency of each schedule.

---

## Note

- Before a UDP-echo entity is configured, the rtr responder command needs to be configured on the destination end to set it as the responder. Note that the scheduling result will be incorrect if the responder is not configured.
- 

### 113.3.6 Configure the FLOW-statistics Entity to Detect Interface Traffic Flow

#### Network Requirements

- A FLOW-statistics entity is used on Device1 to detect interface vlan2 traffic flow.

#### Network Topology

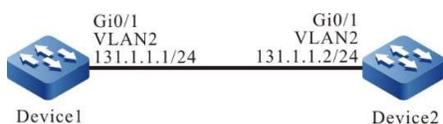


Figure 113-5 Network Topology for Configuring a FLOW-Statistics Entity

#### Configuration Steps

Step 1: Configure IP addresses for the ports. (Omitted)

Step 2: Configure the FLOW-statistics entity on Device1 and add the attribute parameters.

#Configure Device1.

```
Device1#config terminal
Device1(config)#rtr enable
Device1(config)#rtr 1 flow-statistics
Device1(config-rtr-flowsta)#flow-statistics interface vlan 2 interval 60
Device1(config-rtr-flowsta)#number-of-history-kept 255
Device1(config-rtr-flowsta)#exit
```

#View the entity parameters.

```
Device1#show rtr entity 1
-----
ID:1      name:flow-statistics1      Created:TRUE
*****type:FLOWSTATISTICS*****
CreatedTime:THU OCT 25 09:57:43 2012
LatestModifiedTime:THU OCT 25 09:58:03 2012
Times-of-schedule:0
Alarm-type:none
Threshold-of-inputPkt:200000000 direction:be
Threshold-of-inputFlow:200000000 direction:be
Threshold-of-outputPkt:200000000 direction:be
Threshold-of-outputFlow:200000000 direction:be
Interface: vlan2
Statistics-interval:60(s)
Number-of-history-kept:255
Periods:1
Status:DEFAULT
-----
```

The results show that the entity parameters are consistent with the configuration.

Status: DEFAULT indicates that the entity status is DEFAULT.

Step 3: Invoke the defined FLOW-statistics entity and define attribute parameters of the schedule.

#Configure Device1.

```
Device1(config)#rtr schedule 1 entity 1 start now ageout 100 life 600 repeat 10
```

Step 4: Check the result.

1) When there is received data traffic on interface vlan2.

#View the status of an entity.

```
Device1#show rtr entity 1
-----
ID:1      name:flow-statistics1      Created:TRUE
*****type:FLOWSTATISTICS*****
CreatedTime:THU OCT 25 09:57:43 2012
LatestModifiedTime:THU OCT 25 09:58:03 2012
Times-of-schedule:2
Time-of-last-schedule:THU OCT 25 10:02:11 2012
Alarm-type:none
Threshold-of-inputPkt:200000000 direction:be
Threshold-of-inputFlow:200000000 direction:be
Threshold-of-outputPkt:200000000 direction:be
Threshold-of-outputFlow:200000000 direction:be
```

```
Interface: vlan 2
Statistics-interval:60(s)
Number-of-history-kept:255
Periods:1
Status:REACHABLE
-----
```

Status: REACHABLE indicates that the entity is reachable, i.e., there are data packets in/out of the vlan2 interface.

2) When there is no input/output data traffic on interface vlan2.

#View the status of an entity.

```
Device1#show rtr entity 1
-----
ID:1      name:flow-statistics1      Created:TRUE
*****type:FLOWSTATISTICS*****
CreatedTime:THU OCT 25 09:57:43 2012
LatestModifiedTime:THU OCT 25 09:58:03 2012
Times-of-schedule:5
Time-of-last-schedule:THU OCT 25 10:05:11 2012
Alarm-type:none
Threshold-of-inputPkt:200000000 direction:be
Threshold-of-inputFlow:200000000 direction:be
Threshold-of-outputPkt:200000000 direction:be
Threshold-of-outputFlow:200000000 direction:be
Interface: vlan 2
Statistics-interval:60(s)
Number-of-history-kept:255
Periods:1
Status:UNREACHABLE
-----
```

Status: UNREACHABLE indicates that the entity is unreachable when there is no input/output traffic on interface vlan2.

#View the history records.

```
Device1#show rtr history 1
-----
ID:1      Name:flow-statistics1      CurHistorySize:5      MaxHistorysize:255
History recorded as following:
THU OCT 25 10:05:11 2012
    Input pkt:0      (packets/s),Input flow:0      (bits/s),
    Output pkt:0      (packets/s),Output flow:0      (bits/s)
THU OCT 25 10:04:11 2012
    Input pkt:209      (packets/s),Input flow:214000      (bits/s),
    Output pkt:0      (packets/s),Output flow:0      (bits/s)
THU OCT 25 10:03:11 2012
    Input pkt:8460      (packets/s),Input flow:8663000      (bits/s),
    Output pkt:0      (packets/s),Output flow:0      (bits/s)
THU OCT 25 10:02:11 2012
    Input pkt:8460      (packets/s),Input flow:8663000      (bits/s),
    Output pkt:0      (packets/s),Output flow:0      (bits/s)
THU OCT 25 10:01:12 2012
    Input pkt:6456      (packets/s),Input flow:6610000      (bits/s),
    Output pkt:0      (packets/s),Output flow:0      (bits/s)
-----
```

The history records provide details about the rate (number-based and bit-based) of the input and output interface vlan2 for each schedule.

---

## Note

- The reachability of the FLOW-statistics entity is defined as follows: When the entity is in scheduling, and there is traffic flow in the IN or OUT direction of the interface, the entity status is REACHEABLE, otherwise, it is UNREACHABLE.
- 

### 113.3.7 Configuring an ICMP-Echo Ipv6 Entity to Detect Network Communication

#### Network Requirements

- The ICMP-echo ipv6 entity is used on Device1 to detect the network communication from Device1 to Device3.

#### Network Topology



Figure 113-7 Network Topology for Configuring an ICMP-Echo Ipv6 Entity

#### Configuration Steps

- Step 1: Configure the IPV6 address and route of each interface to enable communication between Device1 and Device3. (Omitted)
- Step 2: Configure an ICMP-echo ipv6 entity and add attribute parameters.

#### #Configure Device1.

```
Device1#configure terminal
Device1(config)#rtr enable
Device1(config)#rtr 1 icmpv6echo
Device1(config-rtr-icmpv6echo)#set 2136::2 5 70 2 12 extend 2135::1 0 TRUE
Device1(config-rtr-icmpv6echo)#alarm-type log
Device1(config-rtr-icmpv6echo)#number-of-history-kept 255
Device1(config-rtr-icmpv6echo)#threshold-pktLoss 10 direction be
Device1(config-rtr-icmpv6echo)#threshold-rtt 1000 direction be
Device1(config-rtr-icmpv6echo)#exit
```

#### #View the parameters of an ICMP-echo ipv6 entity.

```
Device1#show rtr entity 1
-----
ID:1      name:Icmpv6Echo1      Created:TRUE
*****type:ICMPV6ECHO*****
CreatedTime:Tue Sep 17 10:05:52 2019
LatestModifiedTime:Tue Sep 17 10:21:06 2019
```

```

Times-of-schedule:0
TargetIpv6:2136::2
Transmit-packets:5
Totally-send-packets:0
Packet-size:70
Timeout:2(s)
Alarm-type:log
Threshold-of-rtt:1000(ms) direction:be
Threshold-of-packet-loss:10 direction:be
Number-of-history-kept:255
Periods:1
Extend parameters:
sourceIpv6:2135::1 tos:0 Verify-data:TRUE
In-scheduling:FALSE
Schedule frequency:12(s)
Status:DEFAULT

```

---

The results show that the entity parameters are consistent with the configuration.

In-scheduling: FALSE indicates that the entity is not scheduled.

Status: DEFAULT indicates that the entity status is DEFAULT.

---

## Note

- When an entity is not scheduled, its status is DEFAULT; when an entity is scheduled, if the entity is reachable, its status is REACHABLE, if it is unreachable, its status is UNREACHABLE.
- 

Step 3: Schedule a defined ICMP-echo ipv6 entity, and define attribute parameters of the schedule.

### #Configure Device1

```
Device1(config)#rtr schedule 1 entity 1 start now ageout 20 life forever
```

Step 4: Check the result.

1) When the network communication from Device1 to Device3 is normal.

### #View the status of an entity.

```
Device1#show rtr entity 1
```

```

-----
ID:1      name:Icmpv6Echo1      Created:TRUE
*****type:ICMPV6ECHO*****
CreatedTime:Tue Sep 17 10:05:52 2019
LatestModifiedTime:Tue Sep 17 10:21:06 2019
Times-of-schedule:2
Time-of-last-schedule:Tue Sep 17 10:24:08 2019
TargetIpv6:2136::2
Transmit-packets:5
Totally-send-packets:10
Packet-size:70
Timeout:2(s)
Alarm-type:log

User manual
Release 1.0 01/2022

```

```

Threshold-of-rtt:1000(ms) direction:be
Threshold-of-packet-loss:10 direction:be
Number-of-history-kept:255
Periods:1
Extend parameters:
sourceipv6:2135::1  tos:0  Verify-data:TRUE
In-scheduling:TRUE
Schedule frequency:12(s)
Status:REACHABLE
-----

```

In-scheduling: TRUE indicates that the entity is in scheduling.

Status: REACHABLE means that the entity status is reachable, that is, the network communication from Device1 to Device3 is normal.

1) When the network communication from Device1 to Device3 fails.

Since the entity parameters are configured with the alarm mode as log, an alarm message will be printed when the threshold value is reached or exceeded, as follows:

```
%SLA-4:Rtr 1 (ICMPV6ECHO) rtt [9000ms] was exceeded(>=) threshold [1000ms].
```

#View the status of an entity.

```

Device1#show rtr entity 1
-----
ID:1      name:Icmpv6Echo1      Created:TRUE
*****type:ICMPV6ECHO*****
CreatedTime:Tue Sep 17 10:05:52 2019
LatestModifiedTime:Tue Sep 17 10:21:06 2019
Times-of-schedule:21
Time-of-last-schedule:Tue Sep 17 10:28:08 2019
TargetIpv6:2136::2
Transmit-packets:5
Totally-send-packets:105
Packet-size:70
Timeout:2(s)
Alarm-type:log
Threshold-of-rtt:1000(ms) direction:be
Threshold-of-packet-loss:10 direction:be
Number-of-history-kept:255
Periods:1
Extend parameters:
sourceipv6:2135::1  tos:0  Verify-data:TRUE
In-scheduling:TRUE
Schedule frequency:12(s)
Status:UNREACHABLE
-----

```

In-scheduling: TRUE indicates that the entity is in scheduling.

Status: UNREACHABLE means that the entity status is unreachable, that is, the network communication from Device1 to Device3 fails.

#View the history records.

```

Device1#show rtr history 1
-----
ID:1 Name:Icmpv6Echo1 CurHistorySize:4 MaxHistorySize:255
History recorded as following:
Tue Sep 17 10:24:42 2019
  PktLoss:5 ,Rtt:invalid

```

```

Tue Sep 17 10:24:29 2019
  PktLoss:1 ,Rtt:400 (ms)
Tue Sep 17 10:24:17 2019
  PktLoss:0 ,Rtt:1 (ms)
Tue Sep 17 10:24:05 2019
  PktLoss:0 ,Rtt:0 (ms)

```

---

The history records provide details about the packet loss and latency of each schedule; an invalid Rtt indicates that there is a failure in the network causing the network to be unreachable.

### 113.3.8 Configure TRACK to Coordinate with SLA

#### Network Requirements

- TRACK is in coordination with SLA. The validity of static routes on Device1 is determined on the basis of entity status.

#### Network Topology



Figure 113-8 Network Topology for Configuring TRACK to Coordinate with SLA

#### Configuration Steps

- Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)
- Step 2: Configure IP addresses for the ports. (Omitted)
- Step 3: On Device1, configure the ICMP-echo entity to detect the network communication from Device1 to Device2, and add the entity to the entity group.

#### #Configure Device1.

```

Device1#config terminal
Device1(config)#rtr enable
Device1(config)#rtr 1 icmpecho
Device1(config-rtr-icmpecho)#set 110.1.0.2 5 70 2 12 extend 110.1.0.1 0 true false
Device1(config-rtr-icmpecho)#number-of-history-kept 255
Device1(config-rtr-icmpecho)#exit
Device1(config)#rtr group 1
Device1(config-rtr-group)#member 1
Device1(config-rtr-group)#exit

```

- Step 4: Define TRACK, and associate it with SLA.

#### #Configure Device1.

```

Device1(config)#track 1
Device1(config-track)#rtr 1

```

Step 5: Add a static route and associate it with TRACK.

#Configure Device1.

```
Device1(config)#ip route 192.0.0.0 255.255.255.0 110.1.0.2 track 1
```

Step 6: Schedule the entity and checking the validity of the static route.

#Configure Device1.

```
Device1(config)#rtr schedule 1 group 1 start now ageout 100 life forever
```

Step 7: Check the result.

1) When the network communication from Device1 to Device2 is normal.

#View the status of an entity group.

```
Device1#show rtr group 1
-----
ID:1      name:rtrGroup1  Members schedule interval:0
Option: AND  Status:REACHABLE
*****
type:SINGLE  Entity Id :1
```

The entity group status is REACHEABLE.

#View the route of network segment 192.0.0.0/24 in the routing table of 'Device1.

```
Device1#show ip route 192.0.0.0
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

S 192.0.0.0/24 [1/10] via 110.1.0.2, 00:00:09, vlan2
```

The result shows that there is a route to the network segment 192.0.0.0/24, indicating that the static route is determined to be valid when the entity group status is RECHABLE.

1) When the network communication from Device1 to Device2 fails.

#View the status of an entity group.

```
Device1#show rtr group 1
-----
ID:1      name:rtrGroup1  Members schedule interval:0
Option: AND  Status:UNREACHABLE
*****
type:SINGLE  Entity Id :1
```

The entity group status is UNREACHEABLE.

#View the route of network segment 192.0.0.0/24 in the routing table of 'Device1.

```
Device1#show ip route 192.0.0.2
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
```

D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

The result shows that there is no route to the network segment 192.0.0.0/24, indicating that the static route is determined to be invalid when the entity status is UNREACHABLE.

### 113.3.9 Configure TRACK to Coordinate with ICMP-Echo Ipv6

#### Network Requirements

- TRACK is in coordination with icmp-echo ipv6. The validity of static routes on Device1 is determined on the basis of entity status.

#### Network Topology



Figure 113-6 Network Topology for Configuring TRACK to Coordinate with Icmp-Echo Ipv6

#### Configuration Steps

Step 1: Configure IP addresses for the ports. (Omitted)

Step 2: On Device1, configure the ICMP-echo ipv6 entity to detect the network communication from Device1 to Device2, and add the entity to the entity group.

#### #Configure Device1.

```
Device1#config terminal
Device1(config)#rtr enable
Device1(config)#rtr 1 icmpv6echo
Device1(config-rtr-icmpv6echo)# set 2135::2 5 70 2 12 extend 2135::1 0 FALSE
Device1(config-rtr-icmpv6echo)#number-of-history-kept 255
Device1(config-rtr-icmpv6echo)#exit
Device1(config)#rtr group 1
Device1(config-rtr-group)#member 1
Device1(config-rtr-group)#exit
```

Step 3: Define TRACK, and associate it with SLA.

#### #Configure Device1.

```
Device1(config)#track 1
Device1(config-track)#rtr 1
Device1(config-track)#exit
```

Step 4: Add a static route and associate it with TRACK.

#Configure Device1.

```
Device1(config)#ipv6 route 2136::/64 2135::2 track 1
```

Step 5: Schedule an entity group.

#Configure Device1.

```
Device1(config)#rtr schedule 1 group 1 start now ageout 20 life forever
```

Step 6: Check the result.

1) When the network communication from Device1 to Device2 is normal.

#View the status of an entity group.

```
Device1#show rtr group 1
```

```
-----  
ID:1      name:rtrGroup1    Members schedule interval:0  
Option: AND  Status:REACHABLE  
*****  
type:SINGLE  Entity Id :1
```

The entity group status is REACHEABLE.

#View the route of network segment 2136::/64 in the routing table of Device1.

```
Device1#show ipv6 route 2136::/64  
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS  
U - Per-user Static route  
O - OSPF, OE-OSPF External, M - Management
```

```
S 2136::/64 [1/0]  
via 2135::2 [0], 00:50:17, vlan100  
2135::2 [0], vlan100
```

The result shows that there is a route to the network segment 2136::/64, indicating that the coordinated static route is determined to be valid when the entity group status is RECHABLE.

1) When the network communication from Device1 to Device2 fails.

#View the status of an entity group.

```
Device1#show rtr group 1
```

```
-----  
ID:1      name:rtrGroup1    Members schedule interval:0  
Option: AND  Status:UNREACHABLE  
*****  
type:SINGLE  Entity Id :1
```

The entity group status is UNREACHEABLE.

#View the route of network segment 2136::/64 in the routing table of Device1.

```
Device1#show ipv6 route 2136::/64  
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS  
U - Per-user Static route
```

The result shows that there is no route to the network segment 2136::/64, indicating that the coordinated static route is determined to be invalid when the entity status is UNREACHABLE.

# 114 NTP

---

## 114.1 Overview

NTP (Network Time Protocol) is the standard Internet protocol used to synchronize the time in Internet. NTP is to synchronize the device time to the standard time. Currently, the adopted time standard is UTC (Universal Time Coordinated).

The design of NTP fully considers the complexity of the time synchronization on Internet. NTP provides the strict, practical, and valid mechanism, applicable to the Internet environments with various scales and speeds. NTP not only corrects the present time, but also continuously tracks the time change and can adjust automatically. Even if the network fails, it can maintain the time stability. NTP generates less network overhead and has measures to ensure network security. The adoption of these measures allows NTP to obtain reliable and accurate time synchronization over the Internet.

In practice, an appropriate NTP working mode should be selected according to the network deployment to meet the network clock synchronization requirements under different circumstances. NTP supports the following three working modes:

- Client/Server Mode

In client/server mode, the client sends a clock synchronization packet to the server with the Mode field set at 3 (client mode), and the server automatically enters the server mode after receiving the packet and sends a response packet with the Mode field set at 4 (server mode). The client synchronizes the system clock after receiving the response packet. In this mode, the client can synchronize the clock from the server, while the server cannot synchronize the clock from the client.

- Peer-to-Peer (P2P) Mode

In P2P mode, NTP packets with the Mode field set at 3 (client mode) and 4 (server mode) are first interacted between the active and passive peers. After that, the active peer sends a clock synchronization packet with the Mode field set at 1 (active peer mode) to the passive peer, and the passive peer automatically enters the passive peer mode after receiving the packet and sends a clock synchronization packet with the Mode field set at 2 (passive peer mode). After packet interaction, the P2P mode is established. In this mode, the active and passive peers can synchronize their clocks with each other. If both clocks are already synchronized, the clock with the smaller number of layers prevails.

- Broadcast Mode

In broadcast mode, the broadcast server periodically sends a clock synchronization packet with the Mode field set at 5 (broadcast server mode) to the broadcast address 255.255.255.255, and the broadcast client listens to the broadcast packet from the broadcast server. After the broadcast client receives the first broadcast packet, NTP packets with the Mode field set at 3 (client mode) and 4 (server mode) are interacted between the broadcast client and the broadcast server to obtain the network latency between the broadcast client and the broadcast server. After that, the broadcast client continues to listen for broadcast packets and synchronizes the system clock based on the received broadcast packets.

## 114.2 NTP Function Configuration

Table 114-114 NTP Function Configuration List

Configuration Task	
Configure NTP basic functions.	Configure the NTP client/server mode.
	Configure NTP P2P mode.
	Configure NTP broadcast mode.
Configure NTP optional parameters.	Configuring the NTP reference clock.
	Configure the source interface for NTP packets.
	Configure the sending and receiving control of NTP packets.
	Configure the number of NTP dynamic sessions.
Configure the NTP authentication function.	Configure the NTP client/server mode authentication.

Configuration Task	
	Configure the NTP P2P mode authentication
	Configure the NTP broadcast mode authentication.
Configure the NTP access control.	Configure the NTP access control.

### 114.2.1 Configure NTP Basic Functions

#### Configuration Condition

Before configuring NTP basic functions, do the following tasks:

- Configure the network layer address of the interface so that the network layer is reachable between the NTP clock service requesting end and the clock service delivering end.
- NTP is enabled on the NTP clock service delivering end.

#### Configure the NTP Client/Server Mode

Under the NTP client/server mode, no special configuration is required on the server, but it is necessary to ensure that the server clock is synchronized and the number of clock layers is less than the number of clock layers on the client.

The following configuration is required on the NTP client.

Table 1-2 Configuring the NTP Client

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Specify the NTP server.	<b>ntp server</b> [ <b>vrf</b> <i>vrf-name</i> ] { <i>ip-address</i>   <b>ipv6</b> <i>ipv6-address</i>   <i>domain-name</i> } [ <b>version</b> <i>version-number</i>   <b>key</b> <i>key-number</i>   <b>source</b> <i>interface-name</i> ]*	Mandatory By default, no NTP server is specified.



**Note**

- 
- The *ip-address* parameter is a unicast address and cannot be a broadcast address, a multicast address, or the IP address of this device.
  - The *ipv6-address* parameter is a global unicast address or the Link-Local address, or a multicast address.
  - After specifying the source interface for sending client packets by **source** interface-name, the primary IP address or the first global unicast IPV6 address of the interface will be set as the source IP address for sending client packets. If the configured server address is an IPv6 Link-local address, the source interface must be specified.
  - Multiple servers can be specified by configuring the **ntp server** or **ntp server ipv6** command multiple times, up to a maximum of 64 servers (the sum of ipv4+ipv6+domains) can be specified.
- 

### Configure NTP P2P Mode

When using the NTP P2P mode, there is no need to specifically configure the passive peer, however, you need to ensure that the passive peer can send and receive NTP packets, which can be achieved by configuring the **ntp enable (ipv6)** command on the passive peer or any of the NTP command in "1.2.1 Configuring NTP Basic Functions" to enable NTP.

The following configuration is required on the NTP active peer.

Table 114-114 Configuring the NTP Active Peer

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Specify the NTP passive peer.	<b>ntp peer [ vrf vrf-name ] { ip-address   ipv6 ipv6-address   domain-name } [ version version-number   key key-number   source interface-name ] *</b>	Mandatory By default, no NTP passive peer is specified.

---

### Note

- The *ip-address* parameter is a unicast address and cannot be a broadcast address, a multicast address, or the IP address of this device.
  - The *ipv6-address* parameter is a global unicast address or the Link-Local address, or a multicast address.
  - After specifying the source interface for sending active peer packets by **source interface-name**, the primary IP address or the first global unicast IPV6 address of the interface will
-

---

be set as the source IP address for sending active peer packets. If the configured peer address is an IPv6 Link-local address, the source interface must be specified.

- Multiple passive peers can be specified by configuring the **ntp peer** or **ntp peer ipv6** command multiple times, up to a maximum of 64 passive peers (the sum of ipv4+ipv6+domain) can be specified.
- 

### Configure NTP Broadcast Mode

When using the NTP broadcast mode, both the broadcast server and the broadcast client need to be configured, and the clock of the broadcast server needs to be synchronized and the number of clock layers is less than the number of clock layers of the broadcast client. Since an interface for sending NTP broadcast packets needs to be specified on the broadcast server and an interface for receiving NTP broadcast packets needs to be specified on the broadcast client, the configuration of the broadcast mode can only be performed in the specific interface mode.

The following configuration is required on the NTP broadcast client.

Table 3-4 Configuring the NTP Broadcast Client

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Enable the NTP broadcast client on the interface.	<b>ntp broadcast-client</b>	Mandatory By default, NTP broadcast client is disabled on the interface.

The following configuration is required on the NTP broadcast server.

Table 5-6 Configuring the NTP Broadcast Server

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-

Step	Command	Description
Enable the NTP broadcast server on the interface.	<b>ntp broadcast-server</b> [ <b>key</b> <i>key-number</i>   <b>version</b> <i>version-number</i> ]*	Mandatory  By default, NTP broadcast server is disabled on the interface.

## 114.2.2 Configure NTP Optional Parameters

### Configuration Condition

None

### Configuring the NTP reference Clock

NTP can synchronize system time in two ways:

- Synchronization with local clock: i.e., the local clock is used as the NTP reference clock.
- Synchronization with other clock sources in the network: i.e., using any of the three aforementioned NTP working modes.

Table 7-8 Configuring the Local Clock as the NTP Reference Clock

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the local clock as the NTP reference clock.	<b>ntp master</b> [ <i>stratum-number</i> ]	Mandatory  By default, the local clock is not configured as the NTP reference clock.

### Note

- After configuring the local clock as the NTP reference clock, the NTP cannot synchronize the clock from other clock sources in the network.

- After configuring the local clock as the NTP reference clock, the local device can be used as a clock source to synchronize other devices in the network. Please use this configuration with caution to avoid causing clock errors on other devices in the network.

### Configure the Source Interface for NTP Packets

If the source interface for a NTP packet is configured, the primary IP address of the specified source interface will be selected as the source IP address of the packet when the device actively sends a NTP packet.

Table 9-10 Configuring the Source Interface for the NTP Packet

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the source interface for NTP packets.	<b>ntp source <i>interface-name</i></b>	Mandatory By default, the source interface of a NTP packet is not configured.

### Note

- If the source interface is specified using the command `ntp server` or `ntp peer`, the source interface specified by the command `ntp server` or `ntp peer` is used first.
- If `ntp broadcast` is configured in the interface mode, the source interface for a NTP broadcast packet is the interface on which the above command is configured.
- If the source interface of the specified NTP packet is in the down state, the source address of the default routing interface primary address or the first global unicast address encapsulating `ntp` is restored to send packets.
- If the source interface of the specified NTP packet has no configured address and is in up state, and there is no corresponding `ipv4` or `ipv6` address, the source address of the default routing interface primary address or the first global unicast address encapsulating `ntp` is restored to send the packet.

### Configure the Sending and Receiving Control of NTP Packets

By default, the device does not receive and send all NTP packets. You can enable receiving and sending NTP packets by configuring the sending and receiving control of NTP packets.

Table 11-12 Configuring the Sending and Receiving Control of NTP Packets

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable to receive and send NTP packets.	<b>ntp enable [ipv6]</b>	Mandatory By default, receiving and sending NTP packets is prohibited.

## Note

- After configuring the **no ntp enable** command, all IPV4 NTP packets will be prohibited from being received and sent, and if the **ntp enable** command is configured, receiving and sending IPV4 NTP packets will be enabled.
- After configuring the **no ntp enable ipv6** command, all IPV6 NTP packets will be prohibited from being received and sent. If the **ntp enable ipv6** command is configured, the receiving and sending of IPV6 NTP packets will be enabled.

### Configure the Number of NTP Dynamic Sessions

Set the maximum number of NTP dynamic connections allowed to be established locally by configuring the number of NTP dynamic sessions.

Table 13-14 Configuring the Number of NTP Dynamic Sessions

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Set the maximum number of NTP dynamic connections allowed to be established locally.	<b>ntp max-dynamic-sessions <i>number</i></b>	Mandatory By default, the number of NTP dynamic sessions allowed to be established is 100.

### 114.2.3 Configure the NTP Authentication Function

In some networks with high security requirements, authentication needs to be enabled when running the NTP protocol. By authenticating the interaction packets between the NTP clock service requesting end and the delivering end, it ensures that the clock service requesting end is synchronized to a legitimate time, improving network security.

#### Configuration Condition

Before configuring the NTP authentication function, do the following tasks:

- Configure the network layer address of the interface so that the network layer is reachable between the NTP clock service requesting end and the clock service delivering end.
- NTP is enabled on the NTP clock service delivering end.

#### Configure the NTP Client/Server Mode Authentication

When configuring the NTP client/server mode authentication, you need to enable authentication on both the client and the server, configure the authentication key, set the authentication key as a trusted key, and specify the key associated with the server on the client.

The following configuration is required on the NTP client.

Table 15-16 Configuring NTP Client Authentication

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable the NTP authentication function.	<b>ntp authenticate</b>	Mandatory By default, the NTP authentication function is not enabled.
Configure the authentication key.	<b>ntp authentication-key</b> <i>key-number</i> <b>md5</b> { <b>0</b> <i>plain-key</i>   <b>7</b> <i>cipher-key</i> }	Mandatory By default, no authentication key is configured.
Configure the specified key as a trusted key.	<b>ntp trusted-key</b> <i>key-number</i>	Mandatory By default, no trusted key is specified.

Step	Command	Description
Specify the key associated with the server.	<b>ntp server</b> [ <i>vrf vrf-name</i> ] { <i>ip-address</i>   <i>domain-name</i>   <b>ipv6</b> <i>ipv6-address</i> } [ <b>version</b> <i>version</i>   <b>source</b> <i>interface-name</i> ] <b>key</b> <i>key-number</i>	Mandatory

The following configuration is required on the NTP server.

Table 17-18 Configuring NTP Server Authentication

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable the NTP authentication function.	<b>ntp authenticate</b>	Mandatory By default, the NTP authentication function is not enabled.
Configure the authentication key.	<b>ntp authentication-key</b> <i>key-number</i> <b>md5</b> { <i>0 plain-key</i>   <i>7 cipher-key</i> }	Mandatory By default, no authentication key is configured.
Configure the specified key as a trusted key.	<b>ntp trusted-key</b> <i>key-number</i>	Mandatory By default, no trusted key is specified.

### Note

- The server and client need to be configured with the same authentication key.

### Configure the NTP P2P Mode Authentication

When configuring the NTP peer mode authentication, you need to enable authentication on both active and passive peers, configure the authentication key, set the authentication key as a trusted key, and specify the key associated with the passive peer on the active peer.

The following configuration is required on the NTP active peer.

Table 19-20 Configuring NTP Active Peer Authentication

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable the NTP authentication function.	<b>ntp authenticate</b>	Mandatory By default, the NTP authentication function is not enabled.
Configure the authentication key.	<b>ntp authentication-key</b> <i>key-number</i> <b>md5</b> { <i>0 plain-key</i>   <i>7 cipher-key</i> }	Mandatory By default, no authentication key is configured.
Configure the specified key as a trusted key.	<b>ntp trusted-key</b> <i>key-number</i>	Mandatory By default, no trusted key is specified.
Specify the key associated with the passive peer.	<b>ntp peer</b> [ <i>vrf vrf-name</i> ] <i>ip-address</i>   <i>domain-name</i>   <b>ipv6</b> <i>ipv6-address</i> [ <b>version</b> <i>version</i>   <b>source</b> <i>interface-name</i> ] <b>key</b> <i>key-number</i>	Mandatory

The following configuration is required on the NTP passive peer.

Table 21-22 Configuring NTP Passive Peer Authentication

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable the NTP authentication function.	<b>ntp authenticate</b>	Mandatory By default, the NTP authentication function is not enabled.
Configure the authentication key.	<b>ntp authentication-key</b> <i>key-number</i> <b>md5</b> { <i>0 plain-key</i>   <i>7 cipher-key</i> }	Mandatory By default, no authentication key is configured.

Step	Command	Description
Configure the specified key as a trusted key.	<b>ntp trusted-key</b> <i>key-number</i>	Mandatory By default, no trusted key is specified.

## Note

- Active and passive peers need to be configured with the same authentication key.

### Configure the NTP Broadcast Mode Authentication

When configuring the NTP broadcast mode authentication, you need to enable authentication on both the broadcast client and the broadcast server, configure the authentication key, set the authentication key as the trusted key, and specify the key associated with this broadcast server on the broadcast server.

The following configuration is required on the NTP broadcast client.

Table 23-24 Configuring NTP Broadcast Client Authentication

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable the NTP authentication function.	<b>ntp authenticate</b>	Mandatory By default, the NTP authentication function is not enabled.
Configure the authentication key.	<b>ntp authentication-key</b> <i>key-number</i> <b>md5</b> { <b>0</b> <i>plain-key</i>   <b>7</b> <i>cipher-key</i> }	Mandatory By default, no authentication key is configured.
Configure the specified key as a trusted key.	<b>ntp trusted-key</b> <i>key-number</i>	Mandatory By default, no trusted key is specified.

The following configuration is required on the NTP broadcast server.

Table 25-26 Configuring NTP Broadcast Server Authentication

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable the NTP authentication function.	<b>ntp authenticate</b>	Mandatory By default, the NTP authentication function is not enabled.
Configure the authentication key.	<b>ntp authentication-key</b> <i>key-number</i> <b>md5</b> { <b>0</b> <i>plain-key</i>   <b>7</b> <i>cipher-key</i> }	Mandatory By default, no authentication key is configured.
Configure the specified key as a trusted key.	<b>ntp trusted-key</b> <i>key-number</i>	Mandatory By default, no trusted key is specified.
Enter the interface configuration mode	<b>interface</b> <i>interface-name</i>	-
Specify the key associated with the broadcast server.	<b>ntp broadcast-server</b> [ <b>version</b> <i>version-number</i> ] <b>key</b> <i>key-number</i>	Mandatory

---

 **Note**

- The broadcast server and the broadcast client need to be configured with the same authentication key.
- 

### 114.2.4 Configure the NTP Access Control

#### Configuration Condition

Before configuring the **NTP** access control, do the following tasks:

- Configure the ACL associated with the access control.

#### Configure the NTP Access Control

NTP can restrict access to the local NTP service by associating it with an ACL.

Table 27-28 Configuring NTP Access Control

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the NTP access control.	<b>ntp access-control list</b> <i>access-list-name</i>	Mandatory By default, the NTP access control is not configured.

### 114.2.5 NTP Monitoring and Maintaining

Table 29-30 NTP Monitoring and Maintaining

Command	Description
<b>show ntp associations [ipv6]</b>	Display NTP session information.
<b>show ntp status</b>	Display NTP status information.
<b>snmp-server enable traps ntp [stratum-change   sync-lost   sync-success]*</b>	Enable the Trap function of NTP.

## 114.3 Typical Configuration Example of NTP

### 114.3.1 Configure the NTP IPV4 Server and Client

#### Network Requirements

- Device1 is the NTP server and Device2 is the NTP client.
- Device1 and Device2 are interconnected through their respective interface VLAN2, and are route reachable.
- The NTP server is the clock source and the client gets the clock from the server.

#### Network Topology



Figure 1-2 Network Topology for Configuring NTP Server and Client

### Configuration Steps

Step 1: Configure IP addresses for the interfaces (omitted).

Step 2: Configure the NTP server Device1.

#Enable NTP IPV4 for Device1, configure the time as China Standard Time, local clock as the reference clock, and the number of clock layers at 3.

```
Device1#configure terminal
Device1(config)#ntp enable
Device1(config)#clock timezone BINJING 8
Device1(config)#ntp master 3
Device1(config)#exit
```

Step 3: Configure the NTP client Device2.

#Enable NTP IPV4 for Device2 and configure the time as China Standard Time.

```
Device2#configure terminal
Device2(config)#ntp enable
Device2(config)#clock timezone BINJING 8
```

#Specify the NTP server Device1, and the IP address is 1.0.0.1.

```
Device2(config)#ntp server 1.0.0.1
Device2(config)#exit
```

Step 4: Check the result.

#On the client Device2, execute **show ntp status** command to check the clock synchronization status and other information, indicating that the client and the NTP server Device1 has been synchronized, the number of clock layers is greater than Device1 by 1, which is 4.

```
Device2#show ntp status
Current NTP status information
NTP ipv4 is enabled
NTP ipv6 is disabled
Clock is synchronized, stratum 4, reference is 1.0.0.1
reference time is D442EB0E.432F29BD (01:49:02.262 Tue Nov 06 2012)
```

#Execute the **show clock** command on the client Device2 to check the device clock.

```
Device2#show clock
BEIJING(UTC+08:00) TUE NOV 06 09:49:30 2012
```

## 114.3.2 Configure the NTP IPv4 Server and Multi-Level Client

### Network Requirements

- Device1 is the NTP server, and Device2 and Device3 are the NTP clients.
- Device2 is interconnected with Device1 and Device3 through interface vlan2 and vlan3, respectively, and the routes are reachable.
- Device1 provides the clock for Device2 and Device2 provides the clock for Device3.

### Network Topology



Figure 3-4 Network Topology for Configuring NTP Server and Multi-Level Client

### Configuration Steps

Step 1: Configure IP addresses for the interfaces (omitted).

Step 2: Configure the NTP server Device1.

#Enable NTP IPv4 for Device1, configure the time as China Standard Time, local clock as the reference clock, and the number of clock layers at 3.

```
Device1#configure terminal
Device1(config)#ntp enable
Device1(config)#clock timezone BINJING 8
Device1(config)#ntp master 3
Device1(config)#exit
```

Step 3: Configure the NTP client Device2.

#Enable NTP IPv4 for Device2 and configure the time as China Standard Time.

```
Device2#configure terminal
Device2(config)#ntp enable
Device2(config)#clock timezone BINJING 8
```

#Specify the NTP server Device1 with the IP address 1.0.0.1.

```
Device2(config)#ntp server 1.0.0.1
```

Step 4: Configure the NTP client Device3.

#Configure to enable NTP IPv4 for Device3 and configure the time as China Standard Time.

```
Device3#configure terminal
Device3(config)#ntp enable
Device3(config)#clock timezone BINJING 8
```

#Specify the NTP server Device2 with the IP address 2.0.0.1.

```
Device3(config)#ntp server 2.0.0.1
```

Step 5: Check the results and the clock synchronization information on Device2 and Device3 respectively.

#On the client Device2, execute **show ntp status** command to check the clock synchronization status and other information, indicating that Device2 and the NTP server Device1 has been synchronized, the number of clock layers is greater than Device1 by 1, which is 4.

```
Device2#show ntp status
Current NTP status information
NTP ipv4 is enabled
NTP ipv6 is disabled
Clock is synchronized, stratum 4, reference is 1.0.0.1
reference time is D44CC35E.BAA6A190 (13:02:22.729 Tue Nov 13 2012)
```

#Execute the **show clock** command on the client Device2 to check the device clock.

```
Device2#show clock
BEIJING(UTC+08:00) TUE NOV 13 21:02:24 2012
```

#On the client Device3, execute **show ntp status** command to check the clock synchronization status and other information, indicating that Device3 and Device2 has been synchronized, the number of clock layers is greater than Device2 by 1, which is 5.

```
Device3#show ntp status
Current NTP status information
NTP ipv4 is enabled
NTP ipv6 is disabled
Clock is synchronized, stratum 5, reference is 2.0.0.1
reference time is D44CC365.5CC8C4C8 (13:02:29.362 Tue Nov 13 2012)
```

#Execute the **show clock** command on the client Device3 to check the device clock.

```
Device3#show clock
BEIJING(UTC+08:00) TUE NOV 13 21:02:36 2012
```

### 114.3.3 Configure NTP Server and Client with MD5 Authentication

#### Network Requirements

- Device1 acts as the NTP server, Device2 acts as the NTP client, and both sides are authenticated with the MD5 algorithm.
- Device1 and Device2 are interconnected through their respective interface VLAN2, and are route reachable.
- The NTP server is the clock source and the client gets the clock from the server.

#### Network Topology



Figure 114-114 Network Topology for Configuring NTP Server and Client with MD5 Authentication

### Configuration Steps

Step 1: Configure IP addresses for the interfaces (omitted).

Step 2: Configure the NTP server.

#Enable NTP IPV4 for Device1, configure the time as China Standard Time, local clock as the reference clock, and the number of clock layers at 3.

```
Device1#configure terminal
Device1(config)#ntp enable
Device1(config)#clock timezone BINJING 8
Device1(config)#ntp master 3
Device1(config)#exit
```

Enable authentication.

```
Device1(config)#ntp authenticate
```

#Configure the authentication key serial number as 1, the algorithm as MD5, and the key as admin.

```
Device1(config)#ntp authentication-key 1 md5 0 admin
```

#Configure the key with serial number 1 to be trusted.

```
Device1(config)#ntp trusted-key 1
```

Step 3: Configure the NTP client.

#Enable NTP IPV4 for Device2 and configure the time as China Standard Time.

```
Device2#configure terminal
Device2(config)#ntp enable
Device2(config)#clock timezone BINJING 8
```

#Specify the NTP server for the client, and the IP address is 1.0.0.1.

```
Device2(config)#ntp server 1.0.0.1
```

Enable authentication.

```
Device2(config)#ntp authenticate
```

#Configure the authentication key serial number as 1, the algorithm as MD5, and the key as admin.

```
Device2(config)#ntp authentication-key 1 md5 0 admin
```

#Configure the key with serial number 1 to be trusted.

```
Device2(config)#ntp trusted-key 1
```

Step 4: Check the result.

#On the client Device2, execute **show ntp status** command to check the clock synchronization status and other information, indicating that the client and the NTP server Device1 has been synchronized, the number of clock layers is greater than Device1 by 1, which is 4.

```
Device2#show ntp status
Current NTP status information
NTP ipv4 is enabled
NTP ipv6 is disabled
Clock is synchronized, stratum 4, reference is 1.0.0.1
reference time is D442ECE1.8BB7B219 (01:56:49.545 Tue Nov 06 2012)
```

#Execute the **show clock** command on Device2 to check the device clock.

```
Device2#show clock
BEIJING(UTC+08:00) TUE NOV 06 09:56:52 2012
```

---

## Caution

- The NTP client and the server must have the same authentication serial number and the same key.
- 

### 114.3.4 Configure the NTP IPV4 P2P Mode

#### Network Requirements

- Device1, Device2 and Device3 are interconnected through their respective interfaces and are reachable by route.
- Device1 sets the local clock as the reference clock and the layer number is 3.
- Device2 acts as the NTP client, and set Device1 as the NTP server.
- Device3 sets Device2 as the peer, Device3 as the active peer, and Device2 as the passive peer.

#### Network Topology

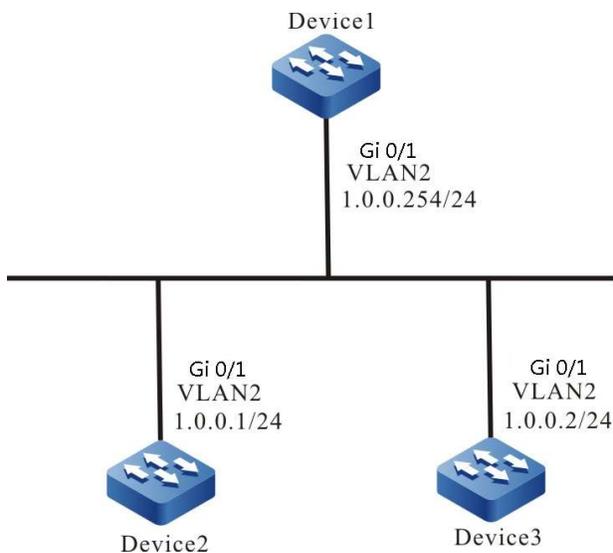


Figure 5-6 Network Topology for Configuring the NTP P2P Mode

### Configuration Steps

Step 1: Configure IP addresses for the ports. (Omitted)

Step 2: Enable NTP IPV4 on Device1, and configure the time as China Standard Time and the number of local clock layers as 3.

```
Device1#configure terminal
Device1(config)#ntp enable
Device1(config)#clock timezone BINJING 8
Device1(config)#ntp master 3
```

Step 3: Device2 specifies Device1 as the NTP server.

#Enable NTP IPV4 on Device2 and configure the time as China Standard Time.

```
Device2#configure terminal
Device2(config)#ntp enable
Device2(config)#clock timezone BEIJING 8
```

#Specify the NTP server IP address as 1.0.0.254.

```
Device2(config)#ntp server 1.0.0.254
```

Step 4: Device3 sets Device2 as the peer.

#Enable NTP IPV4 on Device3 and configure the time as China Standard Time.

```
Device3#configure terminal
Device3(config)#ntp enable
Device3(config)#clock timezone BEIJING 8
```

#Specify the NTP peer IP address as 1.0.0.1.

```
Device3(config)#ntp peer 1.0.0.1
```

Step 5: Check the result.

#Execute the **show ntp status** command on client Device2 to check the clock synchronization status and other information.

```
Device2#show ntp status
Current NTP status information
NTP ipv4 is enabled
NTP ipv6 is disabled
Clock is synchronized, stratum 4, reference is 1.0.0.254
reference time is D8E9785D.221F1F5 (03:09:17.8 Tue Apr 28 2015)
```

Device2 clock layer number is larger than Device1 by 1, which is 4, and the reference clock server address is 1.0.0.254, indicating that the client Device2 and the server Device1 have been synchronized.

#Execute the **show clock** command on the client Device2 to check the device clock.

```
Device2#show clock
BEIJING(UTC+08:00) TUE APR 28 11:10:36 2015
```

#Execute the **show ntp status** command on the active peer Device3 to check the clock synchronization status and other information.

```
Device3#show ntp status
Current NTP status information
NTP ipv4 is enabled
NTP ipv6 is disabled
Clock is synchronized, stratum 5, reference is 1.0.0.1
reference time is D8E9795C.29835CC9 (03:13:32.162 Tue Apr 28 2015)
```

Device3 clock layer number is larger than Device2 by 1, which is 5, and the reference clock server address is 1.0.0.1, indicating that active peer Device3 has been synchronized with passive peer Device2.

#Execute the **show clock** command on the client Device3 to check the device clock.

```
Device3#show clock
BEIJING(UTC+08:00) TUE APR 28 11:16:19 2015
```

### 114.3.5 Configure NTP Broadcast Mode

#### Network Requirements

- Device1, Device2 and Device3 are interconnected through their respective interfaces and are reachable by route.
- Device1 sets the local clock as the reference clock and the layer number is 3.
- Device1 acts as the NTP broadcast server and sends NTP broadcast packets from the vlan2 interface.
- Device2 and Device3 are NTP broadcast clients, listening for NTP broadcast packets on their respective interfaces vlan2.

## Network Topology

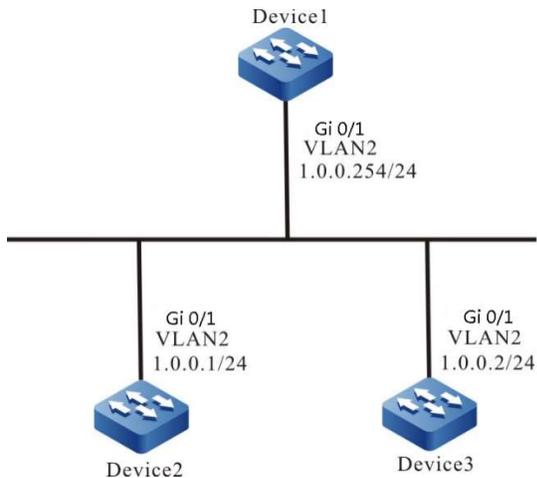


Figure 7-8 Network Topology for Configuring the NTP Broadcast Mode

### Configuration Steps

Step 1: Configure IP addresses for the ports. (Omitted)

Step 2: Device1 sets the local clock as the reference clock and the layer number as 3. Configure Device1 as the NTP broadcast server to send NTP broadcast packets on interface vlan2.

#Enable NTP IPV4 on Device1, and configure the time as China Standard Time and the number of local clock layers as 3.

```
Device1#configure terminal
Device1(config)#ntp enable
Device1(config)#clock timezone BINJING 8
Device1(config)#ntp master 3
```

#Configure Device1 as the NTP broadcast server to send NTP broadcast packets on interface vlan2.

```
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ntp broadcast-server
```

Step 3: Configure Device2 as the NTP broadcast client to listen for NTP broadcast packets on interface vlan2.

```
Device2#configure terminal
Device2(config)#ntp enable
Device2(config)#clock timezone BINJING 8
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ntp broadcast-client
```

Step 4: Configure Device3 as the NTP broadcast client to listen for NTP broadcast packets on interface vlan2.

```
Device3#configure terminal
Device3(config)#ntp enable
Device3(config)#clock timezone BINJING 8
```

```
Device3(config)#interface vlan2
Device3(config-if- vlan2)#ntp broadcast-client
```

Step 5: Check the result.

#Execute the show ntp status command on client Device2 to check the clock synchronization status and other information.

```
Device2#show ntp status
Current NTP status information
NTP ipv4 is enabled
NTP ipv6 is disabled
Clock is synchronized, stratum 4, reference is 1.0.0.254
reference time is D8E97C99.5110D9FE (03:27:21.316 Tue Apr 28 2015)
```

Device2 clock layer number is larger than Device1 by 1, which is 4, and the reference clock server address is 1.0.0.254, indicating that the client Device2 and the server Device1 have been synchronized.

#Execute the show clock command on the client Device2 to check the device clock.

```
Device2#show clock
BEIJING(UTC+08:00) TUE APR 28 11:27:22 2015
```

#Execute the show ntp status command on client Device3 to check the clock synchronization status and other information.

```
Device3#show ntp status
Current NTP status information
NTP ipv4 is enabled
NTP ipv6 is disabled
Clock is synchronized, stratum 4, reference is 1.0.0.254
reference time is D8E97CAC.78F42CA6 (03:27:40.472 Tue Apr 28 2015)
```

Device3 clock layer number is larger than Device1 by 1, which is 4, and the reference clock server address is 1.0.0.254, indicating that the client Device3 and the server Device1 have been synchronized.

#Execute the show clock command on the client Device3 to check the device clock.

```
Device3#show clock
BEIJING(UTC+08:00) TUE APR 28 11:27:41 2015
```

### 114.3.6 Configure the NTP IPV6 Server and Client

#### Network Requirements

- Device1 is the NTP server and Device2 is the NTP client.
- Device1 and Device2 are interconnected through their respective interface VLAN2, and are route reachable.
- The NTP server is the clock source and the client gets the clock from the server.

#### Network Topology

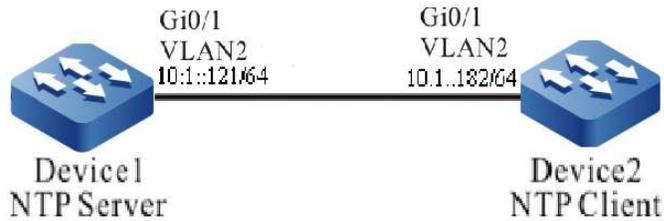


Figure 9-10 Network Topology for Configuring the NTP IPV6 Server and Client

### Configuration Steps

Step 1: Configure the IPv6 address of each interface (omitted).

Step 2: Configure the NTP server Device1.

#Enable NTP IPV6 on Device1, and configure the time as China Standard Time, local clock as the reference clock, and the number of local clock layers as 3.

```
Device1#configure terminal
Device1(config)#ntp enable ipv6
Device1(config)#clock timezone BINJING 8
Device1(config)#ntp master 3
Device1(config)#exit
```

Step 3: Configure the NTP client Device2.

#Enable NTP IPV6 on Device2 and configure the time as China Standard Time.

```
Device2#configure terminal
Device2(config)#ntp enable ipv6
Device2(config)#clock timezone BINJING 8
```

#Specify the NTP server Device1 with the IPV6 address 10:1::121.

```
Device2(config)#ntp server ipv6 10:1::121
Device2(config)#exit
```

Step 4: Check the result.

#On the client Device2, execute **show ntp status** command to check the clock synchronization status and other information, indicating that the client and the NTP server Device1 has been synchronized, the number of clock layers is greater than Device1 by 1, which is 4.

```
Device2#show ntp status
Current NTP status information
NTP ipv4 is disabled
NTP ipv6 is enabled
Clock is synchronized, stratum 4, reference is 10:1::121
reference time is D442EB0E.432F29BD (01:49:02.262 Tue Nov 06 2012)
```

#Execute the **show clock** command on the client Device2 to check the device clock.

```
Device2#show clock
```

### 114.3.7 Configure the NTP IPV6 P2P Mode

#### Network Requirements

- Device1, Device2 and Device3 are interconnected through their respective interfaces and are reachable by route.
- Device1 sets the local clock as the reference clock and the layer number is 3.
- Device2 acts as the NTP client, and set Device1 as the NTP server.
- Device3 sets Device2 as the peer, Device3 as the active peer, and Device2 as the passive peer.

#### Network Topology

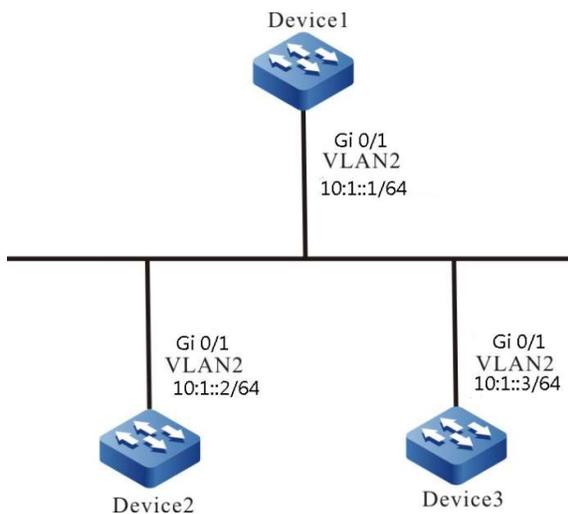


Figure 11-12 Network Topology for Configuring the NTP IPV6 Mode

#### Configuration Steps

Step 1: Configure the IPv6 address for each interface. (Omitted)

Step 2: Enable NTP IPV6 on Device1, and configure the time as China Standard Time and the number of local clock layers as 3.

```

Device1#configure terminal
Device1(config)#ntp enable ipv6
Device1(config)#clock timezone BINJING 8
Device1(config)#ntp master 3
  
```

Step 3: Device2 specifies Device1 as the NTP server.

#Enable NTP IPV6 on Device2 and configure the time as China Standard Time.

```

Device2#configure terminal
Device2(config)#ntp enable ipv6
  
```

```
Device2(config)#clock timezone BEIJING 8
```

#Specify the NTP server IPV6 address as 10:1::1.

```
Device2(config)#ntp server ipv6 10:1::1
```

Step 4: Device3 sets Device2 as the peer.

#Enable NTP IPV6 on Device3 and configure the time as China Standard Time.

```
Device3#configure terminal
Device3(config)#ntp enable ipv6
Device3(config)#clock timezone BEIJING 8
```

#Specify the NTP peer IPV6 address as 10:1::2.

```
Device3(config)#ntp peer ipv6 10:1::2
```

Step 5: Check the result.

#Execute the **show ntp status** command on client Device2 to check the clock synchronization status and other information.

```
Device2#show ntp status
Current NTP status information
NTP ipv4 is disabled
NTP ipv6 is enabled
Clock is synchronized, stratum 4, reference is 10:1::1
reference time is D8E9785D.221F1F5 (03:09:17.8 Tue Apr 28 2015)
```

Device2 clock layer number is larger than Device1 by 1, which is 4, and the reference clock server address is 10:1::1, indicating that the client Device2 and the server Device1 have been synchronized.

#Execute the **show clock** command on the client Device2 to check the device clock.

```
Device2#show clock
BEIJING(UTC+08:00) TUE APR 28 11:10:36 2015
```

#Execute the **show ntp status** command on the active peer Device3 to check the clock synchronization status and other information.

```
Device3#show ntp status
Current NTP status information
NTP ipv4 is disabled
NTP ipv6 is enabled
Clock is synchronized, stratum 5, reference is 10:1::2
reference time is D8E9795C.29835CC9 (03:13:32.162 Tue Apr 28 2015)
```

Device3 clock layer number is larger than Device2 by 1, which is 5, and the reference clock server address is 10:1::2, indicating that active peer Device3 has been synchronized with passive peer Device2.

#Execute the **show clock** command on the client Device3 to check the device clock.

```
Device3#show clock
BEIJING(UTC+08:00) TUE APR 28 11:16:19 2015
```

# 115 Port Mirror

---

## 115.1 Overview

### 115.1.1 Overview

Port mirror, also called SPAN (Switched Port Analyzer), is one management mode used to monitor the data flow of the device port. SPAN includes the local SPAN, remote SPAN and encapsulated remote SPAN.

### 115.1.2 Basic Concepts

#### SPAN Session

SPAN session means to mirror the data flow of one or multiple monitor ports on the device and send to the destination port. The mirrored data flow can be the input data flow and also can be the output data flow or mirror the input and output data flow at the same time. We can configure SPAN for the disabled port and the SPAN session does not take effect, but as long as the related port is enabled, SPAN takes effect.

#### Local SPAN

Local SPAN supports the port mirror on one device. All mirror ports and destination ports are on the same device.

#### Remote SPAN

Remote SPAN, also called RSPAN (Remote Switched Port Analyzer), supports that the mirror port can destination port are not on one device, realizing the remote monitoring across the L2 network. In the specified RSPAN VLAN, each RSPAN Session makes the mirror packets be forwarded in the L2 network. RSPAN includes RSPAN Source Session, RSPAN VLAN, and RSPAN Destination Session. We need to configure RSPAN source session and RSPAN destination session on different devices. When configuring the RSPAN source session, we need to specify one or multiple mirror ports and one RSPAN VLAN. The data mirrored by the monitor port is sent to RSPAN VLAN. To configure RSPAN destination session on another device, we need to specify the destination port and RSPAN VLAN. RSPAN destination session sends RSPAN VLAN data to the destination port.

#### Encapsulated Remote SPAN

Encapsulated Remote SPAN, also known as ERSPAN (Encapsulated Remote Switched Port Analyzer), provides the ability to encapsulate mirrored packets through specific tunnels across Layer-3 network for

data monitoring purposes. When configuring an ERSPAN session, you need to specify one or more monitoring ports, a source IP address, and a destination IP address.

## **VLAN SPAN**

VLAN SPAN supports VLAN mirroring on a single device. Mirror a copy of one or more monitored VLAN streams to the destination port. The mirrored data flow can be the input data flow and also can be the output data flow or mirror the input and output data flow at the same time.

### **Traffic Type**

Traffic type includes Receive (Rx) (the received traffic of the mirror port, Transmit (Tx) (the forwarded traffic of the mirror port, and Both (the received and forwarded traffic of the mirror port).

### **SPAN Source Port**

SPAN source port is also called monitored port. Its data is monitored for network analysis. The monitored data flow can be at the input direction, output direction or both. It can function in different VLANs. The source port can be general port or aggregation group. One source port can only belong to one SPAN session.

### **SPAN Destination Port**

SPAN destination port can only be one separate actual physical port or aggregation group. One destination port can only be used in one SPAN session. The destination port can be general port or aggregation group.

The device supports taking the destination port as the general forwarding port, but for universality and to make the monitored data not be interfered by other data flow, it is suggested to delete the destination port from all VLANs.

---

## **Note**

- The destination port should not be connected to other devices, as this may result in a network loop.
  - The destination port cannot carry any other services.
  - The destination port should be greater than or equal to the bandwidth of the monitored port, otherwise packet loss may occur.
  - The destination port cannot enable LACP (Link Aggregation Control Protocol) or the 802.1X function to avoid mirroring data from being affected.
  - Up to 4 destination ports can be supported for a single session. Depending on the chip, the number of destination ports supported by different boards may vary.
-

## RSPAN VLAN

RSPAN VLAN should be one idle VLAN, specially used by RSPAN. We can select one idle VLAN during configuration, but should ensure that the other devices on the path from the mirror port to the destination port are all configured with the VLAN and add the corresponding ports of the other devices on the path to the VLAN.

## 115.2 SPAN Function Configuration

Table 115-115 SPAN Function Configuration List

Configuration Task	
Configure Local SPAN	Configure a Local SPAN session
Configure RSPAN	Configure RSPAN VLAN
	Configure a RSPAN source session
	Configure a RSPAN destination session
Configure VLAN SPAN	Configure a VLAN SPAN session

### 115.2.1 Configure Local SPAN

Local SPAN is used to analyze the data flow of the local device port.

#### Configuration Condition

None

#### Configure a Local SPAN Session

The Local SPAN session can copy packets received or forwarded by one or more source ports, and forward them from the destination port without affecting the forward of normal service of the source port.

Table 1-2 Configure Local SPAN Sessions

Step	Command	Description
Enter the global configuration mode.	<b>config terminal</b>	-

Step	Command	Description
Configure the source of a Local SPAN session.	<b>monitor session</b> <i>session-number</i> <b>source</b> { <b>interface</b> <i>interface-list</i>   <b>interface link-aggregation</b> <i>link-aggregation-id</i> } [ <b>both</b>   <b>tx</b>   <b>rx</b> ]	Mandatory  By default, the source of a Local SPAN session is not configured.
Configure the destination of a Local SPAN session.	<b>monitor session</b> <i>session-number</i> <b>destination</b> { <b>interface</b> <i>interface-list</i>   <b>interface link-aggregation</b> <i>link-aggregation-id</i> }	Mandatory  By default, the destination of a Local SPAN session is not configured.

---

## Note

- When configuring the source of a session and specifying the port on which mirroring is enabled as the aggregation group, the specified aggregation group should have been created. If the aggregation group has not been created, the configuration fails. Similarly, when configuring a session destination and specifying the mirror packet forwarding port as the aggregation group, the specified aggregation group should also have been created. If the aggregation group has not been created, the configuration fails.
  - The same port cannot be both the source and destination port for the same session.
  - The same port cannot be used in more than one session at the same time.
- 

### 115.2.2 Configure RSPAN

The RSPAN session is used to analyze the data flow from the source port of a remote device that is reachable by the Layer-2 network. An RSPAN session consists of an RSPAN source session and an RSPAN destination session.

#### Configuration Condition

None

#### Configure RSPAN VLAN

An RSPAN session enable mirrored packets to traverse the Layer-2 network by tagging the mirrored packets with RSPAN VLAN tags.

Table 115-115 Configuring RSPAN VLAN

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the VLAN configuration mode	<b>vlan</b> <i>vlan-id</i>	-
Configure VLAN as RSPAN VLAN.	<b>remote-span</b>	Mandatory  By default, no RSPAN VLAN is configured.

### Note

- The RSPAN VLAN should not carry other service traffic, only RSPAN traffic.
- RSPAN VLAN disables the MAC address learning function.
- Do not configure any ports into the RSPAN VLAN except those used to carry RSPAN traffic.

### Configure a RSPAN Source Session

After configuring the RSPAN source session, the mirror packet is tagged with RSPAN VLAN and then forwarded from the destination port of the RSPAN source session.

Table 115-115 Configuring RSPAN Source Sessions

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the source of an RSPAN source session.	<b>monitor session</b> <i>session-number</i> <b>source</b> { <b>interface</b> <i>interface-list</i>   <b>interface link-aggregation</b> <i>link-aggregation-id</i> } [ <b>both</b>   <b>tx</b>   <b>rx</b> ]	Mandatory  By default, the source of an RSPAN source session is not configured.

Step	Command	Description
Configure the destination of an RSPAN source session.	<b>monitor session</b> <i>session-number</i> <b>destination remote vlan</b> <i>vlan-id</i> <b>interface</b> <i>interface-name</i>	Mandatory By default, the destination of an RSPAN source session is not configured.

## Note

- When configuring the source of a session and specifying the port on which mirroring is enabled as the aggregation group, the specified aggregation group should have been created. If the aggregation group has not been created, the configuration fails.
- Specify that the VLAN must be set as an RSPAN VLAN before an RSPAN source session.
- The source and destination of the same session cannot appear at the same port.
- The same port cannot be used in more than one session at the same time.
- The destination port of an RSPAN source session can only be a normal port, not an aggregation group.
- The RSPAN source session supports only one destination port.

### Configure a RSPAN Destination Session

When the RSPAN destination session receives a packet, it identifies the mirror packet based on the RSPAN VLAN tag and forwards the mirror packet to the analysis device.

Table 3-4 Configuring RSPAN Destination Sessions

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the source of an RSPAN destination session.	<b>monitor session</b> <i>session-number</i> <b>source remote vlan</b> <i>vlan-id</i>	Mandatory By default, the source of an RSPAN destination session is not configured.
Configure the destination of an RSPAN destination session.	<b>monitor session</b> <i>session-number</i> <b>destination</b> { <b>interface</b> <i>interface-list</i>	Mandatory

Step	Command	Description
	<b>interface link-aggregation</b> <i>link-aggregation-id</i> }	By default, the destination of an RSPAN destination session is not configured.

## Note

- Specify that the VLAN must be set as an RSPAN VLAN before an RSAPN destination session.
- The same port cannot be used in more than one session at the same time.
- The type of the destination port of an RSPAN destination session should be Hybrid.

### 115.2.3 Configure ERSPAN

An ERSPAN session is used to analyze the data flow from remote device ports that are reachable through the Layer-3 network.

#### Configuration Condition

None

#### Configure an ERSPAN Session

The destination of an ERSPAN source session is used to specify the source IP address, destination IP address, VLAN tag, TTL value, TOS priority of the ERSPAN source session encapsulation, and the mirrored packet can traverse the Layer-3 network after the IP header is encapsulated.

Table 5-6 Configuring ERSPAN Source Sessions

Step	Command	Description
Enter the global configuration mode.	<b>config terminal</b>	-
Configure the source of an ERSPAN source session.	<b>monitor session</b> <i>session-number</i> <b>source</b> { <b>interface</b> <i>interface-list</i>   <b>interface link-aggregation</b> <i>link-aggregation-id</i> } [ <b>both</b>   <b>tx</b>   <b>rx</b> ]	Mandatory  By default, the source of an ERSPAN source session is not configured.

Step	Command	Description
Configure the destination of an ERSPAN source session.	<b>monitor session</b> <i>session-number</i> <b>destination type erspan-source source-ip</b> <i>source-ip-addr</i> <b>destination-ip</b> <i>destination-ip-addr</i> [ <b>vrf</b> <i>vrf-name</i> ] [ <b>vlan</b> <i>vlan-id</i> ][ <b>ttl</b> <i>ttl-value</i> ] [ <b>tos</b> <i>tos-value</i> ]	Mandatory  By default, the destination of an ERSPAN source session is not configured.

## Note

- When configuring a session destination and specifying the mirror packet forwarding port as the aggregation group, the specified aggregation group should also have been created. If the aggregation group has not been created, the configuration fails.
- The same port cannot be used in more than one session at the same time.
- The source IP address must be able to look up the MAC address corresponding to the IP address directly.
- The specified source IP address is configured on the device.
- The next hop-out port must not belong to an aggregation group.
- An ERSPAN session with multiple destination ports is supported. The source IPs can be the same or different, but the destination IPs must be different.

### 115.2.4 Configure VLAN SPAN

The VLAN SPAN session is used to analyze the data flow of the specified VLAN.

#### Configuration Condition

None

#### Configure a VLAN SPAN Session

VLAN SPAN is similar to Local SPAN. The VLAN SPAN session can copy packets received or forwarded by one or more VLAN, and forward them from the destination port without affecting the forward of normal service of the VLAN.

Table 7-8 Configuring VLAN SPAN Sessions

Step	Command	Description
Enter the global configuration mode.	<b>config terminal</b>	-
Configure the source VLAN of a VLAN SPAN session.	<b>monitor session session-number source vlan [ both   tx   rx ]</b>	Mandatory By default, the source VLAN of a VLAN SPAN session is not configured.
Configure the reflector port of a VLAN SPAN session.	<b>monitor session session-number reflector-port interface interface-name</b>	Mandatory By default, the reflector port of a VLAN SPAN session is not configured.
Configure the destination of a VLAN SPAN session.	<b>monitor session session-number destination interface interface-list</b>	Mandatory By default, the destination of a VLAN SPAN session is not configured.

## Note

- The reflector port and destination port of a VLAN SPAN session cannot be a member port of the source VLAN of the VLAN SPAN session.
- The destination port of a VLAN SPAN session can only be a normal port, not an aggregation group.
- The same port cannot be both the reflector and destination port for the same session.
- The source VLAN member ports of a VLAN SPAN session cannot appear in multiple sessions at the same time.
- The reflected port of a VLAN SPAN session cannot carry other service traffic and can only be used by a VLAN SPAN session.
- When configuring the source VLAN for a VLAN SPAN session, if the member ports of the source VLAN already belong to other sessions, the ports will be deleted by the aforementioned sessions.
- The system supports only one VLAN SPAN session.

## 115.2.5SPAN Monitoring and Maintaining

Table 115-115 SPAN Monitoring and Maintaining

Command	Description
<b>show monitor rspan-vlan</b>	Display RSPAN VLAN.
<b>show monitor session</b> { <i>session-number</i>   <b>all</b>   <b>local</b>   <b>remote</b> }	Display the SPAN session configuration information.

## 115.3 Typical Configuration Example of Port Mirroring

### 115.3.1 Configure Local SPAN

#### Network Requirements

- PC1, PC2, and PC3 are connected to Device, and PC1 and PC2 communicate in VLAN 2;
- Configure Local SPAN on Device with the source port as gigabitethernet0/1 and the destination port as gigabitethernet0/3 to enable PC3 to monitor the packets sent and received by Device port gigabitethernet0/1.

#### Network Topology

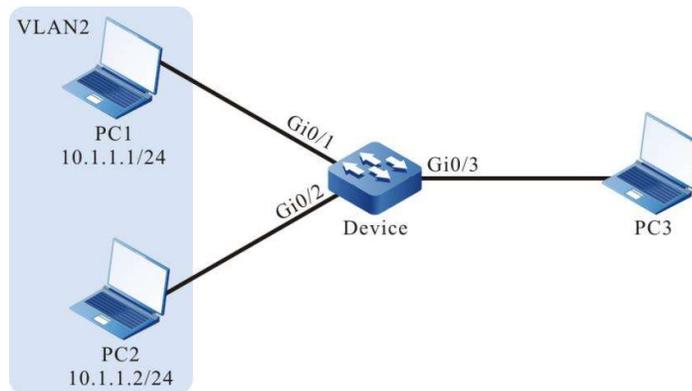


Figure 1-2 Network Topology for Configuring Local SPAN

#### Configuration Steps

Step 1: Configure VLANs and the link type of the ports.

# Create VLAN2 on Device.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the link type of ports gigabitethernet0/1 and gigabitethernet0/2 on Device as Access, allowing the services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/1-0/2
Device(config-if-range)#switchport mode access
Device(config-if-range)#switchport access vlan 2
Device(config-if-range)#exit
```

Step 2: Configure Local SPAN.

#Configure Local SPAN on Device, with the port for mirroring source session as gigabitethernet0/1 and the port for destination session as gigabitethernet0/3.

```
Device(config)#monitor session 1 source interface gigabitethernet 0/1 both
Device(config)#monitor session 1 destination interface gigabitethernet 0/3
```

#Check the Local SPAN session information of on Device.

```
Device#show monitor session all
-----
Session 1
Type      : SPAN Local Session
Destination Interface : gigabitethernet0/3
Source Interface(both): gi0/1
```

Step 3: Check the result.

#When PC1 and PC2 communicate with each other, the packets sent and received on port gigabitethernet0/1 can be captured on PC3.

### 115.3.2Configure RSPAN

#### Network Requirements

- PC1 and PC2 are connected to Device1 and communicate in VLAN2, and PC3 is connected to Device2.
- Configure RSPAN on Device1 and Device2 to enable PC3 to monitor the packets sent and received on Device1 port gigabitethernet0/1 through RSPAN VLAN3.

#### Network Topology

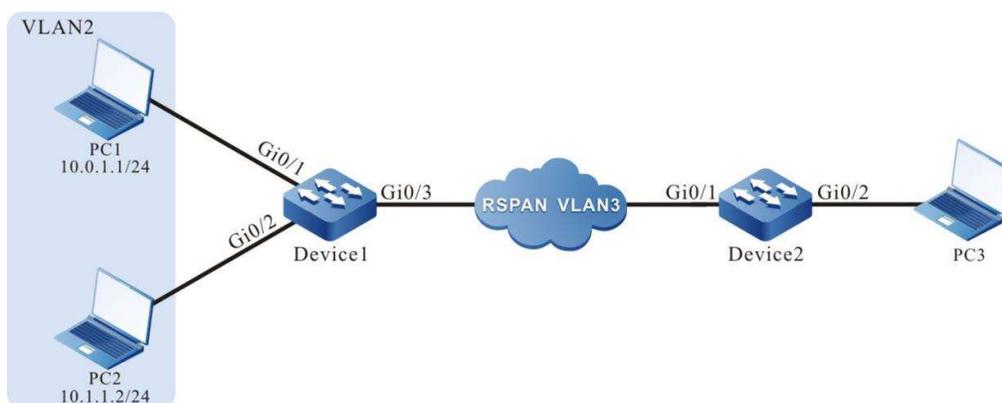


Figure 3-4 Network Topology for Configuring RSPAN

#### Configuration Steps

Step 1: Configure VLANs and the link type of the ports.

#Create VLAN2 on Device1.

```
Device1#configure terminal
Device1(config)#vlan 2
Device1(config-vlan2)#exit
```

#Configure the link type of ports gigabitethernet0/1 and gigabitethernet0/2 on Device1 as Access, allowing the services of VLAN2 to pass.

```
Device1(config)#interface gigabitethernet 0/1-0/2
Device1(config-if-range)#switchport mode access
Device1(config-if-range)#switchport access vlan 2
Device1(config-if-range)#exit
```

#On Device1, configure the link type of port gigabitethernet0/3 as Trunk.

```
Device1(config)#interface gigabitethernet 0/3
Device1(config-if-gigabitethernet0/3)#switchport mode trunk
Device1(config-if-gigabitethernet0/3)#exit
```

#Configure the link type of port gigabitethernet0/1 on Device2 as Trunk.

```
Device2(config)#interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#switchport mode trunk
Device2(config-if-gigabitethernet0/1)#exit
```

#Configure the link type of port gigabitethernet0/2 as Hybrid on Device2.

```
Device2(config)#interface gigabitethernet 0/2
Device2(config-if-gigabitethernet0/2)#switchport mode hybrid
Device2(config-if-gigabitethernet0/2)#exit
```

Step 2: Configure RSPAN on Device1 and Device2.

#Configure VLAN3 as RSPAN VLAN on Device1 and configure port gigabitethernet0/3 to allow services of VLAN3 to pass.

```
Device1(config)#vlan 3
Device1(config-vlan3)#remote-span
Device1(config-vlan3)#exit
Device1(config)#interface gigabitethernet 0/3
Device1(config-if-gigabitethernet0/3)#switchport trunk allowed vlan add 3
Device1(config-if-gigabitethernet0/3)#exit
```

#Configure RSPAN on Device1, with the port for mirroring source session as gigabitethernet0/1 and the port for destination session as gigabitethernet0/3.

```
Device1(config)#monitor session 1 source interface gigabitethernet 0/1 both
Device1(config)#monitor session 1 destination remote vlan 3 interface gigabitethernet 0/3
```

# View RSPAN session information on Device1.

```
Device1#show monitor session all
-----
Session 1
Type      : RSPAN Source Session
RSPAN VLAN   : 3
Destination Interface : gigabitethernet0/3
Source Interface(both): gi0/1
```

#Configure VLAN3 as RSPAN VLAN on Device2 and configure port gigabitethernet0/1 to allow services of VLAN3 to pass.

```
Device2(config)#vlan 3
```

```

Device2(config-vlan3)#remote-span
Device2(config-vlan3)#exit
Device2(config)#interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 3
Device2(config-if-gigabitethernet0/1)#exit

```

#Configure RSPAN on Device2, with the port for mirroring source session as RSPAN VLAN3 and the port for destination session as gigabitethernet0/2.

```

Device2(config)#monitor session 1 source remote vlan 3
Device2(config)#monitor session 1 destination interface gigabitethernet 0/2

```

#View RSPAN session information on Device2.

```

Device2#show monitor session all
-----
Session 1
Type      : RSPAN Destination Session
RSPAN VLAN : 3
Destination Interface : gigabitethernet0/2

```

Step 3: Check the result.

#When PC1 and PC2 communicate with each other, the packets sent and received on Device1 port gigabitethernet0/1 can be captured on PC3.

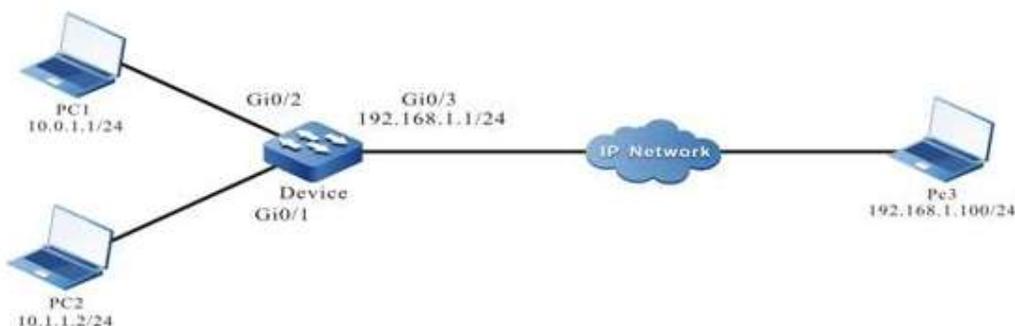
### 115.3.3 Configure ERSPAN

#### 5.3.3.1 Source session

#### Network Requirements

- PC1 and PC2 are connected to Device, and PC1 and PC2 communicate in VLAN 2.
- PC3 communicate with Device through the IP network.
- Configure ERSPAN on Device with the source IP address as 192.168.1.1/24 and the destination IP address as 192.168.1.100/24 to enable PC3 to monitor the packets sent and received on Device port gigabitethernet0/1.

#### Network Topology



## Figure 115-115 Network Topology for Configuring ERSPAN

### Configuration Steps

Step 1: Configure the VLAN, the link type of the port, and the interface address.

#Create VLAN2 and VLAN3 on Device.

```
Device#configure terminal
Device(config)#vlan 2-3
```

#Configure the link type of ports gigabitethernet0/1 and gigabitethernet0/2 on Device as Access, allowing the services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/1-0/2
Device(config-if-range)#switchport mode access
Device(config-if-range)#switchport access vlan 2
Device(config-if-range)#exit
```

#Configure the link type of port gigabitethernet0/3 on Device as Access, allowing the services of VLAN3 to pass.

```
Device(config)#interface gigabitethernet 0/3
Device(config-if-gigabitethernet0/3)#switchport mode access
Device(config-if-gigabitethernet0/3)#switchport access vlan 3
Device(config-if-gigabitethernet0/3)#exit
```

Configure interface IP address on Device.

```
Device(config)#interface vlan 3
Device(config-if-vlan3)#ip address 192.168.1.1 255.255.255.0
Device(config-if-vlan3)#exit
```

Step 2: Configure ERSPAN on Device.

#Configure ERSPAN on the Device, with the port for mirroring the source session as gigabitethernet0/1, the source IP address of the destination session as 192.168.1.1, and the destination IP address as 192.168.1.100.

```
Device(config)#monitor session 1 source interface gigabitethernet 0/1 both
Device(config)#monitor session 1 destination type erspan-source source-ip 192.168.1.1 destination-ip 192.168.1.100
```

#View ERSPAN session information on Device.

```
Device#show monitor session all
-----
Session 1
Type          : ERSPAN Source Session
Destination Interface : gigabitethernet0/3
Source IP Address: 192.168.1.1
Destination IP Address: 192.168.1.100
Source Mac Address: 0001.7a54.5c94
Next Hop Mac Address: 0000.1100.0001
Erspan L2 Vlan:3
Source Interface(both): gi0/1
```

Step 3: Check the result.

#When PC1 and PC2 communicate with each other, the packets sent and received on port gigabitethernet0/1 can be captured on PC3.

### 115.3.4 Configure VLAN SPAN

#### Network Requirements

- PC1, PC2, and PC3 are connected to Device, and PC1 and PC2 communicate in VLAN 2;
- Configure VLAN SPAN on Device with the source vlan as vlan2 and the destination port as gigabitethernet0/3 to enable PC3 to monitor the packets sent and received by the vlan2 interface of Device.

#### Network Topology

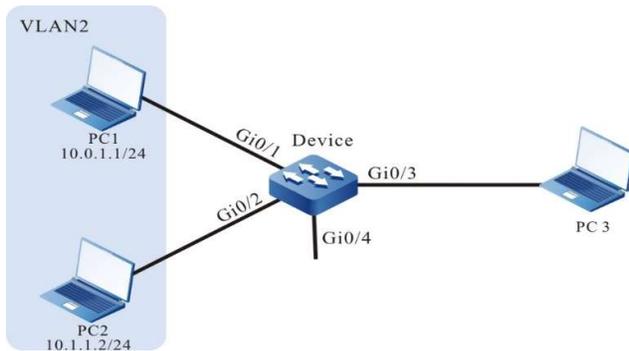


Figure 5-6 Network Topology for Configuring VLAN SPAN

#### Configuration Steps

Step 1: Configure VLANs and the link type of the ports.

# Create VLAN2 on Device.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the link type of ports gigabitethernet0/1 and gigabitethernet0/2 on Device as Trunk, allowing the services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/1-0/2
Device(config-if-range)#switchport mode trunk
Device(config-if-range)# switchport trunk allowed vlan add 2
Device(config-if-range)#exit
```

Step 2: Configure VLAN SPAN.

#Configure VLAN SPAN on Device, with the port for mirroring source session as VLAN2 and the port for destination session as gigabitethernet0/3.

```
Device(config)#monitor session 1 source vlan 2 both
Device(config)#monitor session 1 reflector-port interface gigabitethernet0/4
Device(config)# monitor session 1 destination interface gigabitethernet0/3
Device#show monitor session all
-----
Session 1
Type      : SPAN Local VLAN Session
Destination Interface : gi0/3
Reflector Interface  : gi0/4
Source VLAN(both): 2
```

Step 3: Check the result.

#When PC1 and PC2 communicate with each other, the packets sent and received on VLAN2 can be captured on PC3.

# 116 LLDP

---

## 116.1 Overview

### 116.1.1 Overview of LLDP Protocol

LLDP (Link Layer Discovery Protocol) is the link layer protocol defined in the IEEE 802.1ab standard. It organizes the information of the local device to TLV (Type/Length/Value), encapsulates in LLDPDU (Link Layer Discovery Protocol Data Unit) and sends to the direct-connected neighbor device. Meanwhile, it saves the LLDPDU received from the neighbor device in the standard MIB (Management Information Base) mode. With LLDP, the device can save and manage its own and direct-connected neighbor device information for the network management system to query and judge the link communication status.

### 116.1.2 TLV Type Information

TLV that LLDP can encapsulate includes the basic TLV, organization-defined TLV and MED (Media Endpoint Discovery) TLV. Basic TLV is a group of TLV regarded as the basis of the network device management. Organization defined TLV and MED TLV is the TLV defined by the standard organization and other institutions, used to strengthen the management for the network devices. We can configure whether to release in LLDPDU according to the actual demand.

#### Basic TLV

In basic TLV, there are several types of TLV, which are mandatory for realizing the LLDP function, that is, should be released in LLDPDU, as shown in the following table.

Table 1-2 Basic TLV Description

TLV Type	Description	Whether it must be released
End of LLDPDU TLV	Mark the end of LLDPDU	Yes
Chassis ID TLV	MAC address of the sending device.	Yes
Port ID TLV	Used to identify the port on the sender of LLDPDU. When the device does not send the MED TLV, the content is the port name, and when the MED TLV is scheduled to be sent, the content is the MAC address of the port.	Yes
Time To Live TLV	The time-to-live of local device information on neighbor devices.	Yes
Port Description TLV	Description string of the port.	no
System Name TLV	Name of the device.	no
System Description TLV	DESCRIPTION OF SYSTEM	no
System Capabilities TLV	The main functions of the system, and those of which that are enabled.	no
Management Address TLV	Management address, and the corresponding interface number and OID (Object Identifier). The management address can be a manually configured IP address; if not configured, the primary IP address of the	Yes

TLV Type	Description	Whether it must be released
	management port of the device is selected; if the management port is not configured, the primary IP address of the VLAN through which the interface is allowed is selected; if no primary IP address is configured for any VLAN, the management address value is null. The TLV will be sent by default.	

### Organization-defined TLV

The organization-defined TLV includes the 802.1 organization-defined TLV and 802.3 organization-defined TLV, as shown in the following table.

Table 116-116 802.1 Organization Definition TLV Description

TLV Type	Description	Whether it must be released
Port VLAN ID TLV	Port VLAN ID	no
Port And Protocol VLAN ID TLV	Port and Protocol VLAN ID	no
VLAN Name TLV	Port VLAN Name	no
Protocol Identity TLV	The protocol type supported by the port, the local device does not support sending Protocol Identity TLVs, but can receive TLVs of such type.	no

Table 3-4 802.3 Organizational Definition TLV Description

TLV Type	Description	Whether it must be released
MAC/PHY Configuration/Status TLV	The rate and duplex status of the port; whether the port rate auto-negotiation is supported; whether the auto-negotiation function is enabled; and the current rate and duplex status.	no
Power Via MDI TLV	Power supply capacity of the port.	no
Link Aggregation TLV	Whether the port supports link aggregation and whether it can enable link aggregation.	no
Maximum Frame Size TLV	The maximum frame length supported, taking the configured MTU (Max Transmission Unit) of the port.	no

### MED TLV

MED TLV specific information is shown in the table below.

Table 116-116 MED TLV Description

TLV Type	Description	Whether it must be released
LLDP-MED Capabilities TLV	The MED device type of the device and the type of LLDP MED TLV that can be	no

TLV Type	Description	Whether it must be released
	encapsulated in the LLDPDU.	
Network Policy TLV	Information about the port's VLAN ID, supported applications (such as voice and video), the priority of the application, and the policy used, etc.	no
Extended Power-via-MDI TLV	Power supply capacity of the device.	no
Hardware Revision TLV	Hardware version of the device.	no
Firmware Revision TLV	Firmware version of the device.	no
Software Revision TLV	Software version of the device.	no
Serial Number TLV	Serial number of the device.	no
Manufacturer Name TLV	Manufacturer of the device.	no
Model Name TLV	Module name of the device.	no
Asset ID TLV	Assertion identifiers for the device for directory management and assertion tracking.	no
Location Identification TLV	Location identification information of connected devices for use by other	no

TLV Type	Description	Whether it must be released
	devices in location-based applications.	

### 116.1.3 LLDP Working Mechanism

#### LLDP Working Mode

Four LLDP working modes are supported by port:

- RxTx: It either sends or receives LLDPDU.
- Tx: It only sends LLDPDU.
- Rx: It only receives LLDPDU.
- Disable: It neither sends nor receives LLDPDU.

#### LLDP Sending Mechanism

The LLDP sending mechanism:

- When the port works in the RxTx or Tx mode, regularly send LLDPDU to the neighbor device according to the sending period of the LLDP packet;
- After the port enables the polling function, regularly poll whether the LLDP concerned configuration in the local device changes. If the configuration changes, send LLDPDU at once. To prevent the frequent change of the local information from causing lots of the sent LLDPDU, it is necessary to delay and wait for some time and then continue to send the next LLDPDU when sending one LLDPDU every time.
- When some configuration related with the local device LLDP changes (for example, select the released TLV type), or if finding the configuration change after enabling the polling function, enable the fast sending mechanism, that is, immediately send the LLDPDU of the specified quantity continuously, and then restore the normal LLDP packet sending period.
- When the global LLDP function is disabled or the port enabled with LLDP executes shutdown, adds to the aggregation group, and disables the LLDP, as well as restarts the device, send one LLDPDU with CLOSE TLV to inform the neighbor device.

#### LLDP Receiving Mechanism

When the port works in the RxTx or Rx mode, check the validity of the received LLDPDU and the carried TLV. After passing the validity check, save the neighbor information to the local device and set the age time of the neighbor information at the local device according to the TTL (Time To Live) carried in LLDPDU. If the TTL value in the received LLDPDU is 0, age the neighbor information at once. The storing

capability of the LLDP protocol for the neighbor is limited. If the neighbor reach the threshold, more neighbor advertising packets are dropped and cannot be saved.

## 116.2 LLDP Function Configuration

Table 116-116 LLDP Function Configuration List

Configuration Task	
Configure LLDP basic functions.	Enable the LLDP function globally.
	Enable port LLDP functions.
	Enable the LLDP port-based learning neighbor function.
Configure the LLDP working mode.	Configure the LLDP working mode.
Configure TLV allowed to be released.by LLDP.	Configure the basic TLV allowed to be released.
	Configure the organization-defined TLV that is allowed to be released.
	Configure the MED TLV that are allowed to be released.
Configure the LLDP parameters.	Configure the time-to-live of neighbors.
	Configure the delay time for sending packets.
	Configure the sending period of packets.
	Configure the number of fast packets to be sent.
	Configuration delay of reinitialization.

Configuration Task	
	Configure the inspection cycle of LLDP configuration.

### 116.2.1 Configure LLDP basic functions.

Enable the LLDP function both globally and on ports to allow the LLDP to work properly. The local device gets the neighbor device information by interacting LLDPDUs with other devices.

#### Configuration Condition

None

#### Enable the LLDP Function Globally.

Table 116-116 Enabling the LLDP Function Globally

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable the LLDP function globally.	<b>lldp run</b>	Mandatory By default, the LLDP function is not enabled globally.

#### Enable port LLDP functions.

Table 116-116 Enabling the LLDP Function on Ports

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the L2/L3 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.

Step	Command	Description
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	After you enter the layer-2/3 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enable port LLDP functions.	<b>lldp enable</b>	Optional By default, the LLDP function is enabled on ports.

### Enable the LLDP port-based learning neighbor function.

After configuring the LLDP port-based learning neighbor function, you are able to learn and display neighbors based on a single port of the device. By default, the device learns and displays neighbors based on ports and aggregation group ports.

Table 5-6 Enabling the LLDP Port-Based Learning Neighbor Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable the LLDP port-based learning neighbor function.	<b>lldp mode-ap</b>	Optional By default, this function is disabled.

### 116.2.2 Configure the LLDP working mode.

#### Configuration Condition

None

### Configure the LLDP Working Mode.

Users can set different working modes depending on the role of the device in the network. It is recommended to configure the LLDP working mode as Rx if it is a seed device (central device for network topology collection), otherwise it is recommended to configure the LLDP working mode as Tx.

Table 7-8 Configuring the LLDP Working Mode

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the L2/L3 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2/3 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Configure the LLDP working mode to Rx.	<b>lldp receive</b>	Optional  By default, the LLDP working mode is RxTx.
Configure the LLDP working mode to Tx.	<b>lldp transmit</b>	
Configure the LLDP working mode to RxTx.	<b>lldp receive-transmit</b>	

## 116.2.3 Configure TLV Allowed to Be Released by LLDP

By releasing TLV, you allow neighbor devices to obtain details of local devices.

### Configuration Condition

None

### Configure Basic TLV Allowed to be Released by LLDP

Users can release different basic TLVs according to the needs of the actual application.

Table 9-10 Configuring the Basic TLVs Allowed to be Released by LLDP

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the L2/L3 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2/3 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Configure the Basic TLV Allowed to be Released by LLDP	<b>lldp tlv-select { basic-tlv { all   port-description   system-capability   system-description   system-name } }</b>	Optional  By default, all basic TLVs are allowed to be released.

### Configure Organization-Defined TLVs Allowed to Be Released

Users can release different organization-defined TLV according to the needs of the actual application.

Table 116-116 Configuring the Organization-Defined TLV Allowed to be Released by LLDP

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the L2/L3 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2/3 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Configure the Organization-Defined TLVs Allowed to be Released	<b>lldp tlv-select</b> { <b>dot1-tlv</b> { <b>all</b>   <b>port-vlan-id</b>   <b>protocol-vlan-id</b>   <b>vlan-name</b> }   <b>dot3-tlv</b> { <b>all</b>   <b>link-aggregation</b>   <b>mac-physic</b>   <b>max-frame-size</b>   <b>power</b> } }	Optional  By default, all organization-defined TLVs are allowed to be released.

### Configure MED TLVs Allowed to Be Released by LDDP

Users can release different MED TLVs according to the needs of the actual application.

Table 11-1213 Configuring the MED TLVs Allowed to be Released by LLDP

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Enter the L2/L3 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	After you enter the layer-2/3 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Configure the MED TLVs Allowed to be Released by LDDP	<b>lldp med-tlv-select</b> { <b>all</b>   <b>capability</b>   <b>location-id</b>   <b>elin-address</b> <i>phonenum</i>   <b>network-policy</b>   <b>power-via-mdi</b>   <b>inventory</b> }	Optional By default, not all MED TLVs are allowed to be released.

## 116.2.4 Configure LLDP Parameters

### Configuration Condition

None

### Configure the Time-to-live of Neighbors.

Specify the time-to-live (TTL) of local device information on the neighbor device by configuring the TTL of neighbors, so that the neighbor device can delete the local device information after the local device's TTL expires.

Table 116-116 Configuring Neighbor TTL

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Configure the TTL of local devices on the neighbor devices.	<b>lldp holdtime</b> <i>holdtime-value</i>	Optional By default, the TTL of local devices on the neighbor devices is 120 seconds.

### Configure the Delay Time for Sending Packets

By configuring the packet sending delay time, you can prevent the frequent changes of local information from causing a large number of LLDPDUs to be sent.

Table 116-14 Configuring the Delay Time for Sending Packets

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the delay time for sending LLDP packets.	<b>lldp transmit-delay</b> <i>transmit-delay-value</i>	Optional By default, LLDP packets are sent with a delay time of 2 seconds.

### Configure the Sending Period of Packets

By configuring sending period of a packet, the local device will send a LLDP packet to the neighbor device periodically, so that the information of the local device on the neighbor device will not expire.

Table 15-16 Configuring the Sending Period of Packets

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the sending period of LLDP packets.	<b>lldp transmit-interval</b> <i>transmit-interval-value</i>	Optional By default, the interval of sending a LLDP packet is 30 seconds.

## Configure the Number of Fast Packets to Be Sent

When some configurations related to LLDP of the local device (e.g., the type of TLV selected for releasing) change, or when the polling mechanism checks that the LLDP care configuration information in the local device changes after enabling the polling function, in order to let other devices discover the changes of the local device as soon as possible, the fast sending mechanism will be enabled, i.e., the specified number (default is 3) of LLDPDUs will be sent continuously immediately before reverting to the normal sending period.

Table 17-18 Configuring the Number of Fast Packets Sent

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the number of fast packets to be sent.	<b>lldp fast-count</b> <i>fast-count-value</i>	Optional By default, the number of fast packets sent is 3.

## Configuration Delay of Reinitialization

When the port working mode changes, the port protocol state machine will be re-initialized. To prevent frequent changes of the port working mode from constantly re-initializing the port protocol state machine, you can configure the re-initialization delay time of the port.

Table 19-20 Configuring the Reinitialization Delay

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configuration delay of reinitialization.	<b>lldp reinit</b> <i>reinit-value</i>	Optional By default, the reinitialization delay time is 2 seconds.

## Configure the Inspection Cycle of LLDP Configuration

To enable timely notification of LLDP configuration changes to the neighbor device, you can configure to set the LLDP configuration inspection period.

Table 21-22 Configuring the LLDP Configuration Inspection Period

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the L2/L3 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2/3 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Enable the polling function and configure the polling period.	<b>lldp check-change-interval</b> <i>check-change-interval-value</i>	Optional  By default, the polling function is disabled.

## 116.2.5 LLDP Monitoring and Maintaining

Table 23-24 LLDP Monitoring and Maintaining

Command	Description
<b>clear lldp neighbors</b> [ <b>interface</b> <i>interface-name</i>   <b>interface link-aggregation</b> <i>link-aggregation-id</i> ]	Clear neighbor information.

Command	Description
<b>show lldp neighbors</b> [ <b>detail</b>   <b>interface</b> <i>interface-name</i> [ <b>detail</b> ]   <b>interface link-aggregation</b> <i>link-aggregation-id</i> [ <b>detail</b> ] ]	Display neighbor information.
<b>show lldp neighbors oui</b> [ <b>interface</b> <i>interface-name</i>   <b>interface link-aggregation</b> <i>link-aggregation-id</i> ]	Display neighbor OUI address information and write Voice-VLAN OUI table entry status.
<b>clear lldp statistics</b>	Clear LLDP packet statistics.
<b>show lldp statistics</b> { <b>interface</b> <i>interface-name</i>   <b>interface link-aggregation</b> <i>link-aggregation-id</i> }	Display LLDP packet sending and receiving statistics for the specified port.
<b>show lldp</b>	Display information about LLDP global configuration.
<b>show lldp interface</b> <i>interface-name</i>	Display the LLDP working mode of the specified port and check the polling period for LLDP configuration changes.
<b>show lldp interface link-aggregation</b> <i>link-aggregation-id</i>	Display the LLDP working mode of the specified aggregation group and check the polling period for LLDP configuration changes.
<b>show lldp tlv-select</b> [ <b>interface</b> <i>interface-name</i>   <b>interface link-aggregation</b> <i>link-aggregation-id</i> ]	Used to display configuration information of basic TLVs and organization-defined TLVs.
<b>show lldp voice neighbors</b> [ <b>detail</b>   <b>interface</b> <i>interface-name</i> [ <b>detail</b> ]   <b>interface link-aggregation</b> <i>link-aggregation-id</i> [ <b>detail</b> ] ]	Display voice neighbor information.

## 116.3 Typical Configuration Example of LLDP

### 116.3.1 Configure the Basic Functions of LLDP

#### Network Requirements

- Configure the LLDP function on Device1, Device2 and Device3 respectively to achieve link-layer neighbor discovery.

#### Network Topology



Figure 1-2 Network Topology for Configuring Basic Functions of LLDP

#### Configuration Steps

Step 1: Enable the LLDP function on Device.

#Enable the LLDP function on Device1.

```
Device1#configure terminal
Device1(config)#lldp run
```

#Enable the LLDP function on Device2.

```
Device2#configure terminal
Device2(config)#lldp run
```

#Enable the LLDP function on Device3.

```
Device3#configure terminal
Device3(config)#lldp run
```

Step 2: Configure the LLDP function on ports.

#Enable the LLDP function on port gigabitethernet0/1 of Device1.

```
Device1(config)#interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#lldp enable
Device1(config-if-gigabitethernet0/1)#exit
```

#On ports gigabitethernet0/1 and gigabitethernet0/2 of Device2, enable the LLDP function.

```
Device2(config)#interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#lldp enable
Device2(config-if-gigabitethernet0/1)#exit
Device2(config)#interface gigabitethernet 0/2
Device2(config-if-gigabitethernet0/2)#lldp enable
Device2(config-if-gigabitethernet0/2)#exit
```

#Enable the LLDP function on port gigabitethernet0/1 of Device3.

```
Device3(config)#interface gigabitethernet 0/1
Device3(config-if-gigabitethernet0/1)#lldp enable
Device3(config-if-gigabitethernet0/1)#exit
```

Step 3: Check the result.

#View neighbor information on Device1.

```
Device1#show lldp neighbors

1 neighbor entries in system
Capability codes:
  (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
  (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Index   Local Intf      Hold-time  Capability  Peer Intf   Device ID
1       gi0/1           120       P,R,        gi0/1       Device2

Total entries displayed: 1
```

Device1 discovers neighbor Device2.

#View the information of Device1 neighbor.

```
Device1#show lldp neighbors detail
Neighbor 1:
1. Basic information
Chassis ID       : 0001.7a54.5d0b
Interface ID     : gi0/1
Interface Description : gigabitethernet0/1
System Name      : Device2
System Description : HIT (R) Operating System Software
Copyright (C) 2021 Belden Singapore Pte Ltd.All Rights Reserved.Time Remaining : 111 seconds
System Capabilities : P,R,
Enabled Capabilities : P,R,
Management Addresses : IP,10.0.0.1

2. 802.1 organizationally information
Port VLAN ID : 1
Port And Protocol VLAN ID : 0
VLAN Name Of VLAN 1 : DEFAULT

3. 802.3 organizationally information
Auto Negotiation : Supported, Enabled
OperMau : Speed(1000)/Duplex(Full)
Port Class : PSE
PSE Power : Supported, Enabled
PSE Pairs Control Ability : No
Power Pairs : 1
Power Class : 1
Link Aggregation : Supported, Disabled
Link Aggregation ID : 0
Max Translate Unit : 1824

4. MED organizationally information
Capabilities : Not Supported
Class Type : Not Supported
Application Type : Not Supported
Policy : Not Supported
```

VLAN Tagged : Not Supported  
VLAN ID : Not Supported  
L2 Priority : Not Supported  
DSCP Value : Not Supported  
Location ID : Not Supported  
Power Type : Not Supported  
Power Source : Not Supported  
Power Priority : Not Supported  
Power Value : Not Supported  
HardwareRev : Not Supported  
FirmwareRev : Not Supported  
SoftwareRev : Not Supported  
SerialNum : Not Supported  
Manufacturer Name : Not Supported  
Model Name : Not Supported  
Asset Tracking Identifier : Not Supported  
-----

Total entries displayed: 1

---

## Note

- Refer to Device1 to view the neighbor information of Device2 and Device3.
- 

# 117 SNMP

---

## 117.1 Overview

SNMP (Simple Network Management Protocol) is one standard protocol of managing Internet. It ensures that the management information can be transmitted between Network Managing Station and managed device SNMP agent. It is convenient for the system administrator to manage the network system.

SNMP is one application layer protocol in the client/server mode. It mainly includes three parts:

- NMS (Network Management Station) ;
- SNMP agent
- MIB (Management Information Base) 。

The structure set of all managed objects maintained by the device is called MIB. The managed objects are organized according to the hierarchical tree structure. MIB defines the network management information got by one device. To be consistent with the standard network management protocol, each device should use the format defined in MIB to display the information. One subset of IOS ASN.1 defines the syntax for MIB. Each MIB uses the tree structure defined in ASN.1 to organize all available information. Each piece of information is one node with punctuation and each node contains one object ID and one short text description.

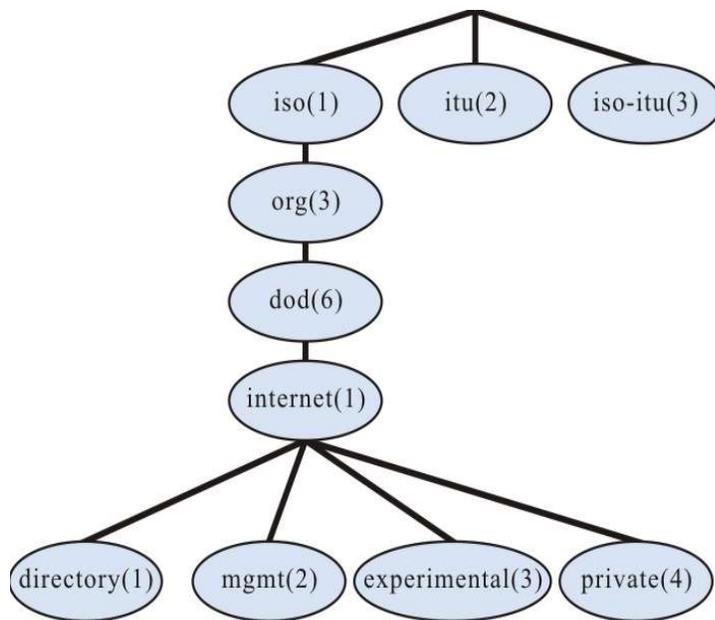


Figure 117-117 Schematic Diagram of the ASN.1 Tree for Network Management

SNMP protocol versions include SNMPv1, SNMPv2, and SNMPv3.

- SNMPv1: The first version of the SNMP protocol. The disadvantages: security problem, bandwidth waste, no communication capability between managers, the protocol only provides the limited operations;
- SNMPv2: It makes some improvement on the basis of SNMPv1, making the functions stronger and the security better;
- SNMPv3: original identity, information integrity and some aspects of re-transmission protect, content confidentiality, authorization and process control, the remote configuration and management capability needed by the above three capabilities;

Therefore, the development of SNMPv3 is centralized on two targets, that is, provide the workable security platform at the enhanced architecture and maintain the consistency of the network management system.

The SNMP protocol mainly includes the following operations:

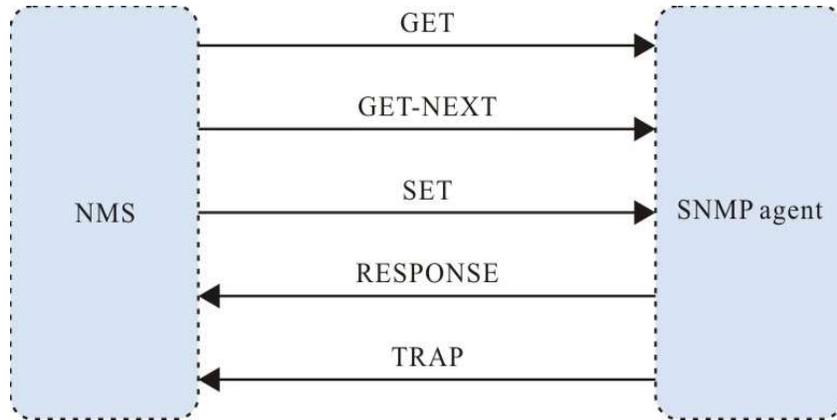


Figure 1-2 SNMP Management Operation Diagram

- Get-request: SNMP network work station gets one or multiple parameters from the SNMP agent.
- Get-next-request: SNMP network work station gets the next parameter of one or multiple parameters from the SNMP agent.
- Get-bulk: SNMP network work station gets the batch parameters from the SNMP agent.
- Set-request: SNMP network work station sets one or multiple parameters of the SNMP agent.
- Get-response: SNMP agent returns one or multiple parameters and it is the responding operation of the SNMP agent for the above three operations.
- Trap: The packet sent by the SNMP agent actively, informing that something happens to the SNMP network work station.

SNMPv1 and SNMPv2 use the authentication name to check whether to have the right to use the MIB object, so only when the authentication name of the network work station is consistent with one authentication name defined in the device, we can manage the device.

The authentication name has the following two attributes:

- Read-only: The read authority of the authorized network work station for all MIB objects of the device;
- Read-write: The read and write authority of the authorized network work station for all MIB objects of the device.

SNMPv3 determines which security mechanism to be adopted to process the data by the security model and the security level. There are three security models: SNMPv1, SNMPv2c, and SNMPv3.

Table 1-2 Supported Security Models and Security Levels

Security Model	Security Level	Certificates	encryption	Description
SNMPv1	NoAuthNoPriv	Authentication name	None	Confirm data legitimacy by authentication name.
SNMPv2c	NoAuthNoPriv	Authentication name	None	Confirm data legitimacy by authentication name.
SNMPv3	NoAuthNoPriv	User Name	None	Confirm data legitimacy by username.
SNMPv3	AuthNoPriv	MD5/SHA	None	Data authentication using HMAC-MD5/HMAC-SHA.
SNMPv3	AuthPriv	MD5/SHA	DES	Data authentication using HMAC-MD5/HMAC-SHA and data encryption using CBC-DES.

## 117.2 SNMP Function Configuration

Table 117-117 SNMP Function Configuration List

Configuration Task	
Configure basic functions of SNMP.	Enable the SNMP service.
	Configure the MIB view.
	Configure the contact information of the administrator.
	Configure the physical location information of the device.

Configuration Task	
Configure SNMPv1/v2.	Configure SNMP community names.
	Configure the SNMP Trap function.
Configure SNMPv3.	Configure an SNMP user group.
	Configure an SNMP user.
	Configure an SNMP advertisement.
	Configure SNMP agent forwarding.

## 117.2.1 Configure Basic Functions of SNMP

### Configuration Condition

None

### Enable the SNMP Service

If the device is enabled with SNMP service, then the device can be configured and managed by the SNMP network management software.

Table 117-117 Enabling the SNMP Service

Step	Command	Description
Enter the global configuration mode.	<b>config terminal</b>	-
Enable the SNMP service.	<b>snmp-server start [ rfc ]</b>	Mandatory The SNMP service is disabled by default.

### Configure the MIB View

By using the view-based access control model, it is determined whether the managed objects associated with an operation are allowed by the view, and only those managed objects that are allowed by the view are allowed to be accessed.

Table 117-117 Configuring the MIB View

Step	Command	Description
Enter the global configuration mode.	<b>config terminal</b>	-
Configure the MIB view.	<b>snmp-server view</b> <i>view-name oid-string</i> { <b>include</b>   <b>exclude</b> }	Mandatory By default, the SNMP view name is Default.
Configure the type of system uptime obtained in the MIB.	<b>snmp-server mib2 sysuptime</b> { <b>snmp-agent-uptime</b>   <b>system-uptime</b> }	Mandatory By default, its type is system-uptime.

### Configure the Contact Information of the Administrator

Administrator contact information is an information node in the SNMP protocol, which can be obtained by the network management software via SNMP.

Table 3-4 Configuring the Contact Information of Administrator

Step	Command	Description
Enter the global configuration mode.	<b>config terminal</b>	-
Configure the contact information of the administrator.	<b>snmp-server contact</b> <i>contact-line</i>	Mandatory

### Configure the Physical Location Information of the Device

The physical location information of the device is an information node in the SNMP protocol, which can be obtained by the network management software via SNMP.

Table 5-6 Configuring the Physical Location of the Device

Step	Command	Description
Enter the global configuration mode.	<b>config terminal</b>	-
Configure the physical location information of the device.	<b>snmp-server location</b> <i>location</i>	Mandatory

## 117.2.2 Configure SNMPv1/v2.

### Configuration Condition

Before configuring SNMPv1/v2, do the following:

- The link layer protocol has been configured to ensure normal communication at the link layer.
- Interface IP addresses have been configured so that neighbor nodes are reachable at the network layer.

### Configure SNMP Community Names

SNMPv1/SNMPv2c uses community-name-based security scheme. An SNMP community name can be regarded as a password between the NMS and SNMP agents, which means the SNMP agent only accepts management operations with the same community name, and SNMPs with different community names will be discarded directly and not be responded.

Table 117-117 Configuring Community Name

Step	Command	Description
Enter the global configuration mode.	<b>config terminal</b>	-
Configure SNMP agent community names.	<b>snmp-server community</b> <i>community-name [ view</i> <i>view-name ] { ro   rw }</i> <i>[ access-list-number  </i> <i>access-list-name]</i>	Mandatory  By default, the community name is public.

### 117.2.3 Configure SNMPv3.

#### Configuration Condition

Before configuring the SNMPv3, do the following:

- The link layer protocol has been configured to ensure normal communication at the link layer.
- Interface IP addresses have been configured so that neighbor nodes are reachable at the network layer.

#### Create an SNMP User Group

When performing control, you can associate certain users with a group. Users in the same group all have the same access rights.

- A group can be configured to associate with a view. There are three types of such views: read-only views, writable views, and advertisement views.
- You can configure the security level of the group and configure whether authentication and encryption are required.

Table 7-8 Creating SNMP User Groups

Step	Command	Description
Enter the global configuration mode.	<b>config terminal</b>	-
Create an SNMP User Group	<b>snmp-server group</b> <i>group-name</i> <b>v3</b> { <b>authnopriv</b>   <b>authpriv</b>   <b>noauth</b> } [ <b>notify</b> <i>notify-view</i>   <b>read</b> <i>read-view</i>   <b>write</b> <i>write-view</i> ]	Mandatory <b>authnopriv</b> means authentication without encryption. <b>authpriv</b> means both authenticated and encrypted. <b>noauth</b> means encryption without authentication.

#### Create an SNMP User

Through the user-based security model for security management, NMSs can only communicate through the SNMP agent using a legitimate user, which of course needs to be configured.

For SNMPv3, you can also specify the security level, authentication algorithm (MD5 or SHA), authentication password, encryption algorithm (DES), and encryption password.

Table 9-10 Configuring Users

Step	Command	Description
Enter the global configuration mode.	<b>config terminal</b>	-
Create an SNMP User	<b>snmp-server user</b> <i>user-name</i> <i>group-name</i> [ <b>remote</b> <i>ip-address</i> <i>port-num</i> ] <b>v3</b> [ <b>auth</b> { <b>md5</b>   <b>sha</b>   <b>SM3</b> } <i>password</i> [ <b>encrypt</b> { <b>des</b>   <b>aes</b>   <b>SM4</b> } <i>password</i> ] ] [ <b>access</b> <i>access-list-number</i>   <i>access-list-name</i>   <b>ipv6</b> <i>access-list-number</i> ]	Mandatory

## Note

- Configure User Security Model (USM)-based SNMPv3 users, saving the authentication and encryption information for each user. Note that the encryption protocol can be configured only after the authentication protocol has been configured.
- For remote users (the so-called remote is relative to the local SNMPv3 entity, if the local SNMPv3 entity has to deal with other SNMPv3 entities, then the other SNMPv3 entities are called remote SNMPv3 entities, which are mentioned in noify and proxy), you also need to specify the IP address and UDP port number of the remote user. When configuring a remote user, please note that you must first configure the engageID of the remote SNMP entity corresponding to that user. In addition, each user must correspond to a group so that a security model and security name can be mapped to a group name through view-based access control.
- When configuring automatic agent forwarding, if you don't know the ip address of the device being proxied, just enter 0.0.0.0 as ip-address. In addition, automatic agent forwarding must be used in combination with the keepalive mechanism.

## Configure an SNMP Advertisement

The types of SNMPv3 advertisement configurations are as follows:

- SNMPv3 advertisement configuration: configure the SNMPv3 advertisement, specify the type of the advertisement message as inform.
- SNMPv3 advertisement filtering configuration: advertisement filtering indicates the filtering used to determine whether an advertisement message should be sent to a destination address.
- SNMPv3 advertisement address mapping table configuration: associate an advertisement address with a filter table.

Table 117-10 Configuring an Advertisement

Step	Command	Description
Enter the global configuration mode.	<b>config terminal</b>	-
Configure an SNMP advertisement.	<b>snmp-server notify notify</b> <i>notify-name taglist inform</i>	Mandatory
Configure SNMP advertisement filtering.	<b>snmp-server notify filter</b> <i>filter-name oid-subtree</i> { <b>exclude</b>   <b>include</b> }	Mandatory  exclude: means to filter out all advertisements of the objects under the MIB subtree.  include: indicates that all objects under the MIB subtree are notified.
Configure SNMP address parameters.	<b>snmp-server</b> <b>AddressParam</b> { <i>address-name</i>   <b>paramIn</b> } <b>v3</b> <i>user-name</i> { <b>noauth</b>   <b>authpriv</b>   <b>authnopriv</b> }	Mandatory
Configure SNMP advertisement filtering mapping table.	<b>snmp-server notify profile</b> <i>filter-name address-param</i>	Mandatory  <i>filter-name</i> : Specify the name of the advertisement filter to be mapped.

Step	Command	Description
		<i>address-param</i> : Specify the name of the address parameter to be mapped.

### Configure SNMP Agent Forwarding

If the NMS cannot directly access a managed SNMP agent, then an intermediate device is required to support agent forwarding. Currently, only SNMPv3 supports agent forwarding.

Table 117-11 Configuring Agent Forwarding

Step	Command	Description
Enter the global configuration mode.	<b>config terminal</b>	-
Configure SNMP remote engine identity.	<b>snmp-server engineID remote</b> <i>ip-address port-num</i> [ <b>vrf</b> <i>vrf-name</i> ] <i>engine-id</i> [ <i>group-name</i> ]	Mandatory Configure the engine identity of an SNMP entity that needs to be forwarded by the agent.
Configure SNMP address parameters.	<b>snmp-server AddressParam</b> [ <i>address-name</i>   <b>paramIn</b> ] <b>v3</b> <i>user-name</i> { <b>noauth</b>   <b>authpriv</b>   <b>authnopriv</b> }	Mandatory
Configure the SNMP advertisement address.	<b>snmp-server TargetAddress</b> <i>target-name ip-address port-num address-param taglist time-out retry-num</i>	Mandatory
Configure SNMP agent forwarding.	<b>snmp-server proxy</b> <i>proxy-name</i> { <b>inform</b>   <b>trap</b>   <b>read</b>   <b>write</b> } { <i>engineId</i>   <b>auto</b> } <i>engineId address-param target-addr</i> [ <i>context-name</i> ]	Mandatory

## 117.2.4 Configure SNMP Trap

Trap is a message sent proactively by the SNMP agent to the NMS to report some specific events. Trap packets are divided into: generic trap and custom trap. Generic trap includes the following: Authentication, Linkdown, Linkup, Coldstart, Warmstart, crc-error, out-packet-error, out-usage-rate, in-packet-error, in-usage-rate, while custom traps are output according to the needs of each module.

Table 117-12 Configuring Trap

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable traps for link interface down or up.	<b>snmp-server enable traps snmp [ linkup   linkdown ]</b>	Mandatory SNMP Trap is not enabled by default.
Enter the interface configuration mode	<b>interface</b> <i>interface-type</i> <i>interface-num</i>	Optional
Configure trap for interface status change.	<b>snmp trap link-status</b>	Optional
Configure trap target host.	<b>snmp-server host</b> { <i>ip-address</i>   <i>host-name</i> } <b>traps</b> { <b>community</b> <i>community-name</i> <b>version</b> { <b>1</b>   <b>2</b> }   <b>user</b> <i>username</i> <b>authnopriv</b>   <b>authpriv</b>   <b>noauth version 3</b> } [ <b>port</b> <i>port-num</i>   <b>vrf</b> <i>vrf-name</i> ]	Mandatory The ip-address needs to be specified as the IP address of the NMS.
Configure the source address of a trap packet.	<b>snmp-server trap-source</b> <i>ip-address</i>	Optional



**Note**

- Since trap information is usually large in quantity, it may occupy device resources and affect device performance. So it is recommended to enable the trap function of specified modules as needed, and avoid enabling all modules' trap.

## 117.2.5SNMP Monitoring and Maintaining

Table 117-13 SNMP Monitoring and Maintaining

Command	Description
<b>show snmp-server</b>	Check information on SNMP protocol packet statistics.
<b>show snmp-server AddressParams</b>	Check information on SNMP-agent address parameters.
<b>show snmp-server community</b>	Check the information of an SNMP-agent community.
<b>show snmp-server contact</b>	Check the contact information of the device's administrator.
<b>show snmp-server context</b>	Check the SNMPv3 contextual environment.
<b>show snmp-server engineGroup</b>	Display information of an SNMP-agent engine group.
<b>show snmp-server engineID</b>	Display information of an SNMP-agent engine ID.
<b>show snmp-server group</b>	Check the information of an SNMP-agent user group.
<b>show snmp-server Host</b>	Display information of an SNMP-agent trap host.
<b>show snmp-server location</b>	Check the information about the location of the device.

Command	Description
<b>show snmp-server notify filter</b>	Display information of SNMP-agent advertisement filtering.
<b>show snmp-server notify notify</b>	Display information of an SNMP-agent advertisement.
<b>show snmp-server notify profile</b>	Display information associated with an SNMP-agent advertisement.
<b>show snmp-server port</b>	Check the port number configured for the SNMP protocol.
<b>show snmp-server proxy</b>	Check the information of SNMP-agent forwarding.
<b>show snmp-server reg-list</b>	Check the module information of SNMP-registered MIBs.
<b>show snmp-server TargetAddress</b>	Check the information of SNMP-agent address table entry.
<b>show snmp-server user</b>	Check the SNMP user information.
<b>show snmp-server view</b>	Check the SNMP view information.

## 117.3 Typical Configuration Example of SNMP

### 117.3.1 Configure an SNMP v1/v2c Proxy Server

#### Network Requirements

- Device acts as an SNMP Agent device that is route reachable to the NMS server.
- The NMS monitors and manages Device through SNMP v1 or SNMP v2c, and Device will actively report to the NMS in case of failure or error.

#### Network Topology

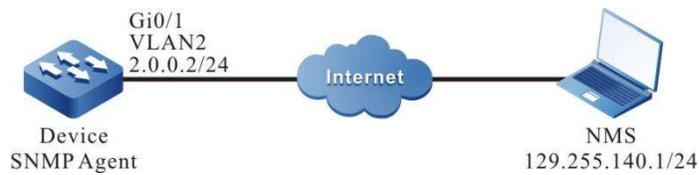


Figure 3-4 Network Topology for Configuring SNMP v1/v2c Proxy Servers

### Configuration Steps

- Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)
- Step 2: Configure IP addresses for the ports. (Omitted)
- Step 3: Enable an SNMP agent on Device and configure the community name of the SNMP.

#### #Configure Device.

Enable the SNMP agent and configure the name of the node view as default, the read-only community name as public, and the read-write community name as public.

```
Device#configure terminal
Device(config)#snmp-server start
Device(config)#snmp-server view default 1.3.6.1 include
Device(config)#snmp-server community public view default ro
Device(config)#snmp-server community public view default rw
```

- Step 4: Configure Device to actively send Trap packets to the Network Management System (NMS) and use the community name public.

#### #Configure Device.

```
Device(config)#snmp-server enable traps
Device(config)#snmp-server host 129.255.140.1 traps community public version 2
```

---

### Note

- The SNMP version specified in the snmp-server host command must be the same as the SNMP version running on the NMS.
- 

- Step 5: Configure the NMS.

#Set the "read-only community name" and the "read-write community name" on the SNMP v1/v2c NMS. In addition, you have to set the "timeout" and "number of retries". Users can query and configure the device through the network management system.

---

## Note

- When using the read-only community name, users can only perform query operations on the device through the network management system.
  - When using the read/write community name, users can query and configure the device through the network management system.
- 

Step 6: Check the result.

#The NMS can query and set the values of certain parameters of Device through the MIB node. The NMS can receive various trap information from Device, such as interface up and down of Device, routing changes caused by network turbulence, etc. Device will generate the corresponding trap information and send it to NMS.

### 117.3.2 Configure an SNMP v3 Proxy Server

#### Network Requirements

- Device acts as an SNMP Agent device that is route reachable to the NMS server.
- The NMS manages Device via SNMP v3.

#### Network Topology

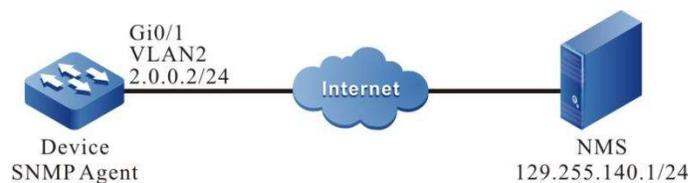


Figure 5-6 Network Topology for Configuring SNMP v3 Proxy Servers

#### Configuration Steps

Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configure IP addresses for the interfaces (omitted).

Step 3: Enable an SNMP agent on Device and configure SNMP v3 basic information.

#Configure Device.

Enable an SNMP agent; configure the name of the node view as default, with access to all objects under node 1.3.6.1.

```
Device#configure terminal
Device(config)#snmp-server start
Device(config)#snmp-server view default1.3.6.1 include
```

Configure user group as public, security level as authpriv, read/write view, and notify view as default; configure user name as public, which belongs to the user group public, authentication algorithm as MD5, authentication password as admin, encryption algorithm as DES, and encryption password as admin.

```
Device(config)#snmp-server group public v3 authpriv read default write default notify default
Device(config)#snmp-server user public public v3 auth md5 admin encrypt des admin
```

Configure the contextual environment as public.

```
Device(config)#snmp-server context public
```

Step 4: Configure the NMS.

#On the NMS using SNMP v3, you need to set the user name and select the security level. According to different security levels, you need to set authentication algorithm, authentication password, encryption algorithm, and encryption password, among others, respectively. In addition, you have to set the "timeout" and "number of retries". Users can query and configure the device through the network management system.

Step 5: Check the result.

#The NMS can query and set the value of certain parameters of Device through the MIB node.

### 117.3.3 Configure SNMP v3 Trap Advertisements

#### Network Requirements

- Device acts as an SNMP Agent device that is route reachable to the NMS server.
- The NMS monitors Device via SNMP v3. Device will actively report to the NMS in case of failure or error.

#### Network Topology



Figure 7-8 Network Topology for Configuring SNMP v3 Trap Advertisements

### Configuration Steps

Step 1: Configure IP addresses for the interfaces (omitted).

Step 2: Enable an SNMP agent on Device and configure SNMP v3 basic information.

#### #Configure Device.

Enable an SNMP agent; configure the name of the node view as default, with access to all objects under node 1.3.6.1.

```
Device#configure terminal
Device(config)#snmp-server start
Device(config)#snmp-server view default 1.3.6.1 include
```

Configure user group as public, security level as authpriv, read/write view, and notify view as default; configure user name as public, which belongs to the user group public, authentication algorithm as MD5, authentication password as admin, encryption algorithm as DES, and encryption password as admin.

```
Device(config)#snmp-server group public v3 authpriv read default write default notify
default
Device(config)#snmp-server user public public v3 auth md5 Admin encrypt des Admin
```

Configure to have Device send all trap messages.

```
Device(config)#snmp-server enable traps
```

Step 3: Configure to have Device send SNMP v3 trap packets to the NMS.

#### #Configure Device.

Configure the SNMP v3 trap user name on the NMS as public and the security level as authpriv.

```
Device(config)#snmp-server host 129.255.140.1 version 3 user public authpriv
```

Step 4: Configure the NMS.

#The NMS needs to be configured with the same username and password as the SNMP agent, run the network management software and listen for UDP port number 162.

Step 5: Check the result.

#The NMS can receive various trap information from Device, such as interface up and down of Device, routing changes caused by network turbulence, etc. Device will generate the corresponding trap information and send it to NMS.

### 117.3.4 Configure SNMP v3 Inform Advertisements

#### Network Requirements

- Device acts as an SNMP Agent device that is route reachable to the NMS server.
- The NMS monitors Device via SNMP v3. Device will actively report to the NMS in case of failure or error.

#### Network Topology

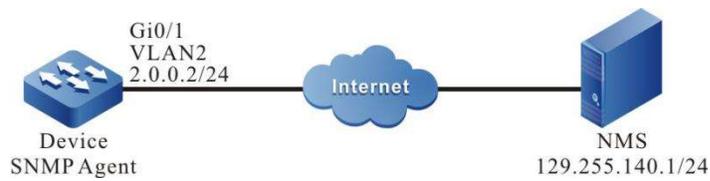


Figure 9-10 Network Topology for Configuring SNMPv3 Advertisements

#### Configuration Steps

Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configure IP addresses for the interfaces (omitted).

Step 3: Enable an SNMP agent on Device and configure SNMP v3 basic information.

#Configure Device.

Enable an SNMP agent; configure the name of the node view as default, with access to all objects under node 1.3.6.1.

```
Device#configure terminal
Device(config)#snmp-server start
Device(config)#snmp-server view default 1.3.6.1 include
```

Configure the user group as group1, the security level as authpriv, and set as default for both read and write view and notify view.

```
Device(config)#snmp-server group group1 v3 authpriv read default write default notify default
```

Configure user name as user2, which belongs to the user group group1, authentication algorithm as MD5, authentication password as admin, encryption algorithm as DES, and encryption password as admin.

```
Device(config)#snmp-server user user2 group1 public v3 auth md5 admin encrypt des admin
```

Configure the contextual environment as public.

```
Device(config)#snmp-server context public
```

Step 4: Configure Device to send advertisement messages to the NMS.

#Configure Device.

Configure the IP address and engineID of remote users, i.e., NMS.

```
Device(config)#snmp-server engineID remote 129.255.140.1 162 bb87654321
```

Configure remote user name as user1, which belongs to the user group group1, authentication algorithm as MD5, authentication password as admin, encryption algorithm as DES, and encryption password as admin.

```
Device(config)#snmp-server user user1 group1 remote 129.255.140.1 162 v3 auth md5 admin encrypt des admin
```

Configure the local address parameter named as param-user1; configure the target address name as target-user1, use the address parameter param-user1, and the target address list name target-user1.

```
Device(config)#snmp-server AddressParam param-user1 v3 user1 authpriv  
Device(config)#snmp-server TargetAddress target-user1 129.255.140.1 162 param-user1 tag-user1 10 3
```

Configure the advertisement entity of notify as notify-user1; configure the filter entity of notify as filter-user1, containing the advertisement of all objects under node 1.3.6.1; configure the advertisement configuration table so that the filter entity filter-user1 is associated with the address parameter param-user1.

```
Device(config)#snmp-server notify notify notify-user1 tag-user1 inform  
Device(config)#snmp-server notify filter filter-user1 1.3.6.1 include  
Device(config)#snmp-server notify profile filter-user1 param-user1
```

Step 5: Configure the NMS.

#On the NMS using SNMP v3, you need to set the user name and select the security level. According to different security levels, you need to set authentication algorithm, authentication password, encryption algorithm, and encryption password, etc., and listen on UDP port number 162.

Step 6: Check the result.

#The NMS can receive various trap information from Device, such as interface up and down of Device, routing changes caused by network turbulence, etc. Device will generate the corresponding trap information and send it to NMS.

## 117.3.5 Configure SNMP v3 Agent Forwarding

### Network Requirements

- Device2 is route reachable to the NMS server.
- Device2 acts as the agenting device, i.e. Agent, and Device1 acts as the device being proxied.
- SNMP v3 is running on both Device1 and Device2.
- The NMS is running SNMP v3. The NMS manages Device1 and Device2 through SNMP v3.

### Network Topology



Figure 11-12 Network Topology for Configuring SNMP v3 Agent Forwarding

### Configuration Steps

- Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)
- Step 2: Configure IP addresses for the interfaces (omitted).
- Step 3: Enable an SNMP agent on the agent device Device2 and configure SNMP v3 basic information.

#### #Configure Device2.

Enable an SNMP agent, configure the name of the node view as default, with access to all objects under node 1.3.6.1.

```
Device2#configure terminal
Device2(config)#snmp-server start
Device1(config)#snmp-server view default 1.3.6.1 include
```

Configure user group as group-local, security level as authpriv, read/write view, and notify view as default; configure user name as user1, which belongs to the user group group-local, authentication algorithm as MD5, authentication password as proxy, encryption algorithm as DES, and encryption password as proxy.

```
Device1(config)#snmp-server group group-local v3 authpriv read default write default notify default
Device1(config)#snmp-server user user1 group-local v3 auth md5 admin encrypt des admin
```

Step 4: Enable an SNMP agent on the device being proxied, i.e. Device1, and configure the SNMP view.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#snmp-server start
Device1(config)#snmp-server view default 1.3.6.1 include
```

Step 5: Configure the information of the proxied device on the agent device Device2.

#Configure Device2.

Configure the IP address of the device being proxied and the engineID.

```
Device2(config)#snmp-server engineID remote 150.1.2.2 161 800016130300017a000137
```

Configure the user group of the proxied device as group-user, the security level as authpriv, and use default for read/write view and notify view.

```
Device2(config)#snmp-server group group-user v3 authpriv read default write default notify default
```

Configure user name as re-user, which belongs to the user group group-user, authentication algorithm as MD5, authentication password as admin, encryption algorithm as DES, and encryption password as admin.

```
Device2(config)#snmp-server user re-user group-user remote 150.1.2.2 161 v3 auth md5 admin encrypt des admin
```

Configure the local address parameter named as plocal; the name of the remote address parameter as puser; configure the target address name as tuser, and use the address parameter puser.

```
Device2(config)#snmp-server AddressParam plocal v3 user1 authpriv
Device2(config)#snmp-server AddressParam puser v3 re-user authpriv
Device2(config)#snmp-server TargetAddress tuser 150.1.2.2 161 puser taguser 10 2
```

Configure the agent forwarding name as proxy-re-user, the operation permission as write, the engineID of the proxied device as 800016130300017a000137, the address parameter used as plocal, and the target address used as tuser; and configure the name of the contextual environment as proxyuser.

```
Device2(config)#snmp-server proxy proxy-re-user write 800016130300017a000137 plocal tuser proxyuser
Device2(config)#snmp-server context proxyuser
```

#Check the engineID information of Device2.

```
Device2#show snmp-server engineID
Local engine ID: 80001613030000000052fd
IPAddress: 150.1.2.2 remote port: 161 remote engine ID: 800016130300017a000137
```



- 
- The enginID of the remote device must be the same as that of the proxied device. The enginID of the device can be viewed with the command `show snmp-server engineID`.
  - The proxied device is listening on UDP protocol and port 161.
- 

Step 6: Perform SNMPV3 related configuration on Device1, the device being proxied.

#Configure Device1.

Configure user group as g1, security level as authpriv, read/write view, and notify view as default; configure user name as re-user, authentication algorithm as MD5, authentication password as admin, encryption algorithm as DES, and encryption password as admin.

```
Device1(config)#snmp-server group g1 v3 authpriv read default write default notify default
Device1(config)#snmp-server user re-user g1 v3 auth md5 admin encrypt des admin
Device1(config)#snmp-server context proxyuser
```

Step 7: Configure the NMS.

#SNMP v3 uses authentication and encryption security mechanism, you need to set the user name and select the security level on the NMS. According to different security levels, you need to set authentication algorithm, authentication password, encryption algorithm, and encryption password, among others, respectively. In addition, you have to set the "timeout" and "number of retries". Users can use the NMS to complete the query and configuration operation of the device. When the proxied device is to be queried or configured, it is also necessary to set the enginID of the agent forwarding to be the enginID of the proxied device on the NMS.

Step 8: Check the result.

#The NMS can query and set the value of certain parameters of Device2 and Device1 through the MIB node.

## 117.4 Overview

One important function of the network management is to monitor the element performances of the network. In the traditional SNMP network management mode, the initiative of the management is mainly mastered by the network management station. Usually, the network management work station regularly polls the data of the device and then measures and analyzes in the network management system, so as to get the desired information of the administrator. In this mode, the network management work station needs to send and receive lots of packets to the network devices. When there are many devices in the network, it causes the additional load for the network. Meanwhile, the network blocking and other factors take various accidents to the running of the network management system. As for this, we put forward the RMON (Remote Network Monitoring) concept.

RMON still requires SNMP protocol support, which is actually a set of MIBs assigned under MIB-2 with the object identifier 1.3.6.1.2.1.16. Compared with other general MIB, RMON adds the calculation at Agent during realizing, that is, put the processing, such as performance statistics in the device. This realizes the distributed processing in the whole network, reducing the disadvantages brought by the polling of the network management work station.

RMON needs to realize lots of calculation functions, so the previous RMON proxy (also called Probe) is acted by a special device, distributed in the network to monitor the corresponding target. With the improvement of the processing capability of the network device, RMON is gradually integrated to the network devices, so as to realize the RMON requirement high-efficiently. However, this also puts forward higher performance requirement for the network devices. After all, the calculations of RMON occupy lots of system resources, reducing the system performance. This is also the additional cost brought by the management, so RMON is mainly realized in the hardware with the network processing capability, such as switching chip.

There are 10 groups of RMON MIB:

- statistics: to measure all Ethernet interfaces of the device, such as broadcast and conflict;
- history: to record the samples of the periodical statistics information that is taken out from the statistics group;
- alarm: to permit the administration Console user to configure the sampling interval and alarm when the values of any counters or integers (recorded by the RMON proxy) exceed the threshold value;
- host: to include the input/output traffics of various types of hosts adhering to the subnet;
- hostTopN: to contain the stored statistics information of hosts, some parameters in the host tables of these hosts are the highest;

- matrix: to indicate the error and utilization information in the form of matrix, so that the operator can use any address pair to search

for information;

- filter: to permit the monitor to monitor the packets matched with the filter;
- capture: The packet capture group creates a set of buffers to store the packets captured from the channel.
- event: to present the table of all events generated by the RMON proxy;
- tokenRing: to maintain the statistic and configuration information of a subnet which is a token ring

## 117.5 RMON Function Configuration

Table 11-12 RMON Function Configuration List

Configuration Task	
Enable the RMON function.	Enable the RMON function.
Configure RMON alarm groups.	Configure RMON alarm instances.
Configure RMON event groups.	Configure RMON to trigger events.
Configure RMON history groups.	Configure RMON history instances.
Configure RMON statistics groups.	Configure the RMON statistics management function.

### 117.5.1 Enable the RMON Function

#### Configuration Condition

None

#### Enable the RMON Function

RMON is enabled to provide the relevant resources for the monitoring function of RMON, and the resources will take effect only after the monitoring group function of RMON is configured.

Table 13-14 Enabling the RMON Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable the RMON function.	<b>rmon</b>	Mandatory

## 117.5.2 Configure RMON Alarm Groups

RMON alarm group function refers to the configuration of multiple alarms, each alarm monitors an alarm instance, and an alarm event is triggered when the alarm instance data value changes beyond the rising threshold or falling threshold during the sampling interval, and the alarm is processed according to the processing method defined by the alarm event group. When the data value continuously exceeds the threshold value, only the first exceedance is alerted.

### Configuration Condition

Before configuring RMON alarm groups, do the following:

- Enable the SNMP agent function.
- Enable the trap function of RMON in SNMP.

### Configure RMON Alarm Instances

Table 15-16 Configuring RMON Alarm Instances

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable the RMON function.	<b>rmon</b>	Optional

Step	Command	Description
Configure RMON alarm groups.	<b>rmon alarm</b> <i>alarm-num</i> <i>OID interval</i> { <b>absolute</b>   <b>delta</b> } <b>risingthreshold</b> <i>rising-threshold</i> [ <i>rising-event</i> ] <b>fallingthreshold</b> <i>falling-threshold</i> [ <i>falling-event</i> ] [ <b>owner</b> <i>owner</i> ]	Mandatory  By default, the alarm trigger event group is 1.  By default, the alarm group is owned by config.

### 117.5.3 Configuring RMON Extended Alarm Groups

RMON extended alarm groups can perform calculations on alarm variables, and then compare the results with the set thresholds to achieve more alarm functions.

#### Configuration Condition

Before configuring RMON alarm groups, do the following:

- Enable the SNMP agent function.
- Enable the trap function of RMON in SNMP.
- Configure a statistics group.

#### Configure RMON Alarm Instances

Table 17-18 Configuring RMON Alarm Instances

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable the RMON function.	<b>rmon</b>	Optional
Configure a statistics group.	<b>rmon statistics ethernet</b> <i>statistics-num</i> <i>OID</i> [ <b>owner</b> <i>owner</i> ]	Mandatory  By default, the statistics group is owned by config.

Step	Command	Description
Configure RMON alarm groups.	<b>rmon prialarm</b> <i>alarm-num</i> <i>WORD interval</i> { <b>absolute</b>   <b>delta</b> } <b>risingthreshold</b> <i>rising-threshold rising-event</i> <b>fallingthreshold</b> <i>falling-threshold falling-event</i> <b>entrytype forever</b> [ <b>ownerowner</b> ]	Mandatory  By default, the alarm group is owned by config.

### 117.5.4 Configure RMON Event Groups

Configure the RMON event group function means configuring multiple events, defining the event number of each event and how it is handled. Events are handled in the following ways: events are recorded in the log, events send TRAP messages to the network management, events are recorded in the log and TRAP messages are sent to the network management without being handled.

#### Configuration Condition

Before configuring an RMON event group, do the following:

- Enable the SNMP agent function.
- Enable the trap function of RMON in SNMP.

#### Configuring RMON to Trigger Events

RMON triggering events is mainly used for event handling when an RMON alarm occurs.

Table 19-20 Configuring RMON to Trigger Events

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable the RMON function.	<b>rmon</b>	Optional
Configure RMON event groups.	<b>rmon event</b> <i>event-num</i> [ <b>description</b> <i>event-</i>	Mandatory

Step	Command	Description
	<i>description</i> / <b>log max-num</b> / <b>owner owner</b> / <b>trap</b> <i>communit</i> ]	By default, the event group is owned by config.

### 117.5.5 Configure RMON History Groups

Configure the RMON history group function means configuring multiple history groups, and the RMON history group stores the subnet data obtained by sampling at a fixed interval. The group consists of a history control table, which defines the subnet interface number being sampled, the size of the sampling interval, and the amount of data sampled each time, and a data table, which stores the various data obtained during the sampling period.

#### Configuration Condition

Before configuring the RMON history group, do the following:

- Enable the SNMP agent function.

#### Configure RMON History Instances

The RMON history group mainly configures information such as the monitoring object of the history control table, the size of the sampling interval, and the quantity of sampled data.

Table 21-22 Configuring RMON History Groups

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable the RMON function.	<b>rmon</b>	Optional
Configure RMON history groups.	<b>rmon history control</b> <i>history-num</i> <i>OID</i> <i>buckets-num</i> [ <b>interval</b> <i>interval</i> ] [ <b>owner</b> <i>owner</i> ]	Mandatory  By default the sampling interval is 1800 seconds.  By default, the history group is owned by config.

## 117.5.6 Configure RMON Statistics Groups

To configure the RMON statistics group function is to configure the statistics of Ethernet interfaces which are the monitoring objects. The statistics group provides a table, each row of which represents the statistics of a subnet, from which the network administrator can obtain various statistics of a segment (the traffic of a segment, the distribution of various types of packets, the number of various types of error packets, the number of collisions, etc.).

### Configuration Condition

Before configuring an RMON statistics group, do the following:

- Enable the RMON function.
- Enable the SNMP agent function.

### Configure the Statistics Management Function

Table 23-24 Configuring the RMON Statistics Management Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable the RMON function.	<b>rmon</b>	Mandatory
Configure RMON statistics groups.	<b>rmon statistics ethernet statistics-num</b> <i>OID</i> [ <b>owner owner</b> ]	Mandatory By default, the statistics group is owned by config.

## 117.5.7 RMON Monitoring and Maintaining

Table 25-26 RMON Monitoring and Maintaining

Command	Description
<b>show rmon alarm</b>	Display the configured RMON alarms in the device.

Command	Description
<b>show rmon alarm supportVariable</b>	Display the monitoring objects supported by RMON in the device.
<b>show rmon event</b>	Display the configured RMON alarm events in the device.
<b>show rmon history</b> { <b>control</b>   <b>ethernet control-num</b> }	Display the configured RMON history groups in the device.
<b>show rmon prialarm</b>	Display the configured RMON extended alarms in the device.
<b>show rmon statistics ethernet</b>	Display the configured RMON statistics groups in the device.

## 117.6 Typical Configuration Example of RMON

### 117.6.1 Configure Basic Functions of RMON

#### Network Requirements

- Device is an RMON agent device that is route reachable to the NMS server.
- Monitoring and management of event groups, alarm groups, history groups, and statistics groups of RMON through NMS.

#### Network Topology



Figure 13-14 Network Topology for Configuring Basic Functions of RMON

#### Configuration Steps

Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configure IP addresses for the ports. (Omitted)

Step 3: Configure an SNMP agent.

#Enable the SNMP agent to configure the name of the node view as default, and the read-only community name as public.

```
Device#configure terminal
Device(config)#snmp-server start
Device(config)#snmp-server view default 1.3.6.1 include
Device(config)#snmp-server community public view default ro
```

#Enable the SNMP Trap function to configure the destination address of the Trap packet and the community name to be used.

```
Device(config)#snmp-server enable traps
Device(config)#snmp-server host 129.255.151.1 traps community public
```

Step 4: Configure the RMON event groups, alarm groups, history groups, and statistics groups of Device.

#Enable an RMON agent.

```
Device(config)#rmon
```

#Configure the event group named Event with the serial number 1 to log packets in the inbound direction of port gigabitethernet0/1.

```
Device(config)#rmon event 1 description gigabitethernet0/1_in_octes log 100 trap public
```

#Configure the alarm event group named Alarm, with the monitoring object as ifInOctets.1. Configure relative value sampling, with the sampling interval to be 10 seconds. Configure the rising and falling thresholds to 100, and configure the event triggered by the threshold to be event 1.

```
Device(config)#rmon alarm 1 ifInOctets.1 10 delta risingthreshold 100 1 fallingthreshold 100 1 owner 1
```

#Configure the statistics group of RMON.

```
Device(config)#rmon statistics ethernet 1 ifIndex.1
```

#Configure the history group of RMON.

```
Device(config)#rmon history control 1 ifIndex.1 10
```

---

## Note

- The instance index number ifInOctets.1 corresponds to port gigabitethernet0/1 on the device. You can display all Layer-2 port snmp index values by show interface switchport snmp ifindex, show interface snmp ifindex to display all Layer-3 port snmp index value, show interface switchport XXXX snmp ifindex to show the specified Layer-2 port snmp index value, show interface XXXX snmp ifindex to show the

---

specified Layer-3 port snmp index value.

- The object instance index number for remote monitoring needs to be read from the interface table ifEntry in MIB-2.
- 

Step 5: Configure the NMS.

#Set the "read-only community name", "timeout" and "number of retries" on the SNMP v1/v2c NMS.

Step 6: Check the result.

#Check the RMON event group table entry configuration for Device.

```
Device#sh rmon event
Event 1 is active, owned by config
Description : gigabitethernet_0/1_in_octes
Event firing causes: log and trap, last fired at 11:38:07
```

Current log entries:

logIndex	logTime	Description
1	11:38:07	gigabitethernet_0/1_in_octes

#Check the RMON alarm table entry configuration for Device.

```
Device#show rmon alarm
Alarm 1 is active, owned by 1
Monitoring variable: ifInOctets.1, Sample interval: 10 second(s)
Taking samples type: delta, last value was 4225
Rising threshold : 100, assigned to event: 1
Falling threshold : 100, assigned to event: 1
```

#Check the RMON event group table entry configuration for Device.

```
Device#sh rmon statistics ethernet
```

-----  
Ethernet statistics table information:

```
Index: 1
Data Source: ifIndex.1
Owner: config
Status: Valid
```

-----  
ifIndex.1 statistics information:

```
-----
DropEvents:0
Octets: 26962295
Pkts:252941
BroadcastPkts:156943
MulticastPkts:62331
CRCAlignErrors:51
UndersizePkts:0
OversizePkts:0
Fragments:0
Jabbers:0
Collisions:0
Pkts64Octets:167737
Pkts65to127Octets:47962
```

```
Pkts128to255Octets:22497
Pkts256to511Octets:9967
Pkts512to1023Octets:4032
Pkts1024to1518Octets:745
```

#Check the RMON history group table entry configuration for Device.

```
Device#show rmon history control
-----
RMON history control entry index: 1
  Data source: IfIndex.1
  Buckets request: 10
  Buckets granted: 2
  Interval: 1800
  Owner: config
  Entry status: Valid
-----
```

#The NMS can query the History, Event and Statistics information in Device through the MIB node.

The NMS is able to receive trap information for alarm events from Device. For example, when the rate of change of traffic in the inbound direction of the monitored interface is greater than the rising threshold or less than the falling threshold, Device will generate the corresponding trap message and send it to the NMS.

## 117.7 Overview

CWMP (CPE WAN Management Protocol, i.e. user-side device WAN management protocol) is a protocol developed by BroadBandForum.org (formerly DSL Forum) for managing and configuring CPE (Customer Premise Equipment user-side equipment), also known as TR-069, which defines a common protocol framework, message specification, management method and data model for managing client-side equipment in carrier Internet broadband access networks.

CWMP can be described as a data framework model that describes the communication between end devices like broadband routers and ACS (Auto-Configuration Server) for remote and centralized configuration management of user-side devices (e.g., broadband routers, switches, Internet gateway devices, set-top boxes, etc.) from the network side.

The CWMP protocol is an application layer protocol that sits on top of IP, which makes the protocol widely applicable with no restrictions on access methods. CPE based on access methods such as ADSL (Asymmetrical Digital Subscriber Loop), Ethernet, and PON (Passive Optical Network) can use this protocol. The TR069-based system architecture is shown in the figure below. The end-to-end architecture of the CWMP protocol has three features:

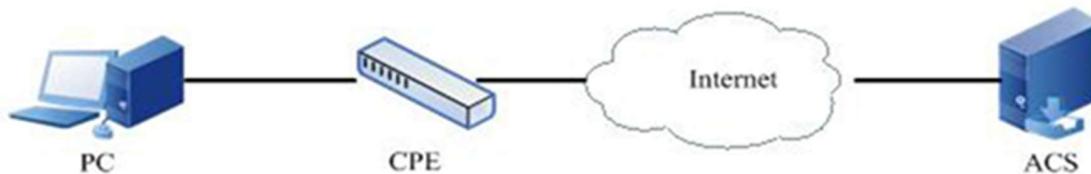


Figure 117-117 TR069-Based System Architecture

1. It has a resilient connection model where both CPE and ACS can trigger the establishment of connections, avoiding the need to maintain connections between CPE and ACS.
  2. Automatic discovery between CPE and ACS is possible.
  3. ACS can dynamically configure and monitor CPE.

For user-side devices, CWMP accomplishes the following four main tasks:

1. Automatic configuration and dynamic service configuration for CPE. For ACS, each CPE can flag itself in the protocol (e.g., model, version, etc.), and depending on the rules that can be set, ACS can issue a configuration for a specific CPE or for a group of CPEs. The CPE can automatically request configuration information in the ACS after power on, and the ACS can also initiate configuration at any desired

moment. This feature enables "zero-configuration installation" of CPE or dynamic change of service parameters controlled from the network side.

2. Management of version files and configuration files of CPE. CWMP provides the management and download of version files and configuration files in CPE. ACS can identify the version number of the user device, decide whether to update the software version of the user device remotely, and be able to know whether the update was successful when it is completed. CPE is under the control of ACS to perform backup by uploading configuration files and restore by downloading configuration files.

3. Remote upgrade of CPE device configuration. It is a function initiated by ACS to remotely upgrade the configuration of CPE. Currently, ACS remotely upgrades the device's configuration by segmenting the CPE's configuration down.

4. Implement security management of device ports: Through CWMP's custom RPC method (remote procedure call), the security management of device ports can be performed, including the functions of disabling, enabling, auto-binding, un-auto-binding, 802.1x based ports, disabling 802.1x, etc. of device ports.

---

## Warning

- The device with 16M Flash will not be powered off or rebooted during the version upgrade via CWMP, and it is necessary to ensure the correct version of the upgrade, otherwise the system may not start.

---

## Note

- When the device is operating in the VST mode, the device does not support the CWMP function.
- 

## 117.8 CWMP Function Configuration

Table 117-117 CWMP Function Configuration List

Configuration Task	
	Enter the CWMP configuration mode.

Configuration Task	
Configure basic functions of CWMP.	Enable a CWMP agent.
	Configure ACS server-related information.
	Configure the WAN device interface.
	Configure CWMP to send INFORM packets periodically.
	Configure the period for CWMP to send INFORM packets.
	Configure the CWMP file download function.
	Configure the CWMP file breakpoint transfer function.
	Configure CWMP provision code.
Configure CWMP authentication and encryption functions.	Configure CWMP authentication information.
	Configure ACS certificates for CWMP.
	Configure ACS certificate fingerprints for CWMP.
Configure CWMP extended functions.	Configure CWMP to specify the source IP address.
	Configure CWMP link backup.

### 117.8.1 Configure Basic Functions of CWMP

#### Configuration Condition

You need to enter the global configuration mode before configuring the basic functions of a CWMP agent.

#### Enter the CWMP Configuration Mode

Enter the CWMP agent configuration mode before performing any CWMP-agent-related configuration.

Table 117-117 Entering the CWMP Configuration Mode

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the CWMP agent configuration mode.	<b>cwmp agent</b>	Mandatory

### Enable a CWMP Agent

If the CWMP agent is enabled on the device, then the device can interact with ACS through the CWMP agent to achieve remote configuration and management of the device.

Table 117-117 Enabling CWMP Proxy Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the CWMP agent configuration mode.	<b>cwmp agent</b>	Mandatory
Enable a CWMP agent.	<b>enable</b>	Mandatory By default, the CWMP agent is disabled.

### Configure ACS Server-related Information

By configuring ACS-related information, including the connection address of the ACS server, the device can communicate with the ACS server.

Table 117-117 Configuring ACS Server-Related Information

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Enter the CWMP agent configuration mode.	<b>cwmp agent</b>	Mandatory
Enable a CWMP agent.	<b>enable</b>	Mandatory By default, the CWMP agent is disabled.
Configure ACS related information.	<b>management server url</b> <i>url-string</i>	Mandatory By default, the device is not configured with the relevant parameters of ACS. For non-encrypted methods, the <i>url-string</i> uses the http protocol; for encrypted methods, the <i>url-string</i> uses the https protocol.
Configure the user name for the device to initiate a connection to the ACS.	<b>management server</b> <i>user-name</i>	Optional By default, the device is not configured with the relevant parameters of ACS. If the user name is not configured on the ACS, it can be configured without.
Configure the password corresponding to the user name for the device to initiate a connection to the ACS.	<b>management server</b> <i>password</i>	Optional By default, the device is not configured with the relevant parameters of ACS. If the user name and corresponding password are not configured on the

Step	Command	Description
		ACS, the configuration can be done without.

### Configure the WAN Device Interface

Specify the interface as the default WAN device interface in the interface mode. If no default WAN device is specified, the CWMP agent cannot send the Inform packet to connect to the ACS server.

Table 27-28 Configuring WAN Device Interfaces

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Access to the Layer-3 interface to be used.	<b>interface</b> <i>interface-name</i>	Mandatory Must be configured under the Layer-3 interface.
Configure the default WAN device.	<b>cwmp wan default</b>	Mandatory By default, no wan device interface is specified for the CWMP agent.

### Note

- Failure to specify a default WAN device will result in CWMP not being able to send Inform packets to connect to the ACS. This is because when organizing Inform packets, you need to clearly know the parameter name of the WAN device connected to the external network in the current system and the IP address of this device interface.
- When a Layer-3 interface is specified as the default WAN device, if no WAN IP address is configured in the CWMP mode and an IP address is configured for this interface, the connection request URL is generated using this interface IP address.

### Configure CWMP to Send INFORM Packets Periodically

By configuring CWMP to send Inform packets periodically, the device can send Inform packets to the ACS periodically, and the ACS will process them accordingly according to the pre-configuration after receiving the Inform packets from the device.

Table 29-30 Configuring CWMP to Send INFORM Packets Periodically

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the CWMP agent configuration mode.	<b>cwmp agent</b>	Mandatory
Enable a CWMP agent.	<b>enable</b>	Mandatory By default, the CWMP agent is disabled.
Configure CWMP to send INFORM packets periodically.	<b>enable inform</b>	Mandatory By default, the function of CWMP sending INFORM packets periodically is enabled.

### Configure the Period for CWMP to Send INFORM Packets

After configuring to enable CWMP periodically send Inform packets, you can configure the period for the CWMP agent to send Inform packets. The default sending period is 43200 seconds (12 hours).

Table 117-117 Configuring the Period for CWMP to Send Inform Packets

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the CWMP configuration mode.	<b>cwmp agent</b>	Mandatory
Enable a CWMP agent.	<b>enable</b>	Mandatory

Step	Command	Description
		By default, the CWMP agent is disabled.
Configure CWMP to send INFORM packets periodically.	<b>enable inform</b>	Mandatory By default, the function of CWMP sending INFORM packets periodically is enabled.
Configure the period for CWMP to send INFORM packets.	<b>inform interval</b> <i>inform-interval</i>	Mandatory By default, the time interval for the device to automatically and periodically send inform packets is 43200 seconds.

---

### Note

- If you have configured to enable the CWMP agent to send Inform packets without configuring the sending period for the Inform packets, CWMP sends Inform packets to ACS at the default period of 43200 seconds (12 hours).
  - After modifying the periodic sending interval of Inform packets, the modified value will take effect only after the expiration of the last interval. If you need the modification to take effect immediately, you can do so by restarting the CWMP agent, where enable and no enable are described in the relevant sections of the CWMP command manual.
- 

### Configure the CWMP File Download Function

When you need the CWMP agent to support file download for version file and configuration file, you need to configure the file download function of the CWMP agent in advance.

Table 117-117 Configuring CWMP File Download

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the CWMP agent configuration mode.	<b>cwmp agent</b>	Mandatory
Enable a CWMP agent.	<b>enable</b>	Mandatory By default, the CWMP agent is disabled.
Configure the CWMP file download function.	<b>enable download</b>	Mandatory By default, CWMP does not enable the file download function.

### Configure the CWMP File Breakpoint Transfer Function

When you configure the file download function of CWMP, you can configure this function when you need CWMP to support the breakpoint transfer function of files.

Table 117-117 Configuring CWMP File Breakpoint Transfer

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the CWMP agent configuration mode.	<b>cwmp agent</b>	Mandatory
Enable a CWMP agent.	<b>enable</b>	Mandatory By default, the CWMP agent is disabled.
Configure the CWMP file download function.	<b>enable download</b>	Mandatory

Step	Command	Description
		By default, CWMP does not enable the file download function.
Configure the CWMP file breakpoint transfer function.	<b>enable download resume</b>	Mandatory By default, CWMP does not enable the file breakpoint transfer function.

## Note

- Before you can configure the breakpoint transfer function of CWMP files, you must configure the file download function of CWMP. If there is no configuration file download function at the beginning, the file breakpoint transfer will not work even if the file renewal function is configured later.

### Configure CWMP Provision Code

The provision code used to configure the CWMP, is used to mark the basic service information provided by the CWMP.

Table 117-117 Configuring the Provision Code of CWMP

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the CWMP agent configuration mode.	<b>cwmp agent</b>	Mandatory
Enable a CWMP agent.	<b>enable</b>	Mandatory By default, the CWMP agent is disabled.

Step	Command	Description
Configure CWMP provision code.	<b>provision code</b> <i>provision-code</i>	Mandatory By default, CWMP is not configured with a provision code.

## 117.8.2 Configure CWMP Authentication and Encryption Functions

### Configuration Condition

Before configuring the authentication and encryption functions of CWMP, do the following:

- The basic configuration of a CWMP agent has been completed, including the enabling configuration of the CWMP agent and the information configuration of the ACS proxied by the CWMP agent.
- When configuring the encryption function, prepare the certificate and import it manually when needed.

### Configure the Authentication Function of CWMP

When the ACS needs to initiate a connection to the device, the CWMP agent needs to be configured to authenticate the connection request from the ACS for security reasons.

Table 117-117 Configure the Authentication Function of CWMP

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the CWMP agent configuration mode.	<b>cwmp agent</b>	Mandatory
Enable a CWMP agent.	<b>enable</b>	Mandatory By default, the CWMP agent is disabled.
Configure the user name for the CPE to	<b>connection request username</b> <i>user-name</i>	Mandatory

Step	Command	Description
authenticate connection requests from the ACS.		By default, no user name is configured.
Configure the password for the CPE to authenticate connection requests from the ACS.	<b>connection request password</b> <i>password</i>	Mandatory By default, no password is configured.

### Configure ACS Certificates for CWMP

For security reasons, when the device connects to ACS by HTTPS, it is necessary to specify the location of the server-side certificate so that the validity of the ACS-side certificate can be verified with this certificate.

Table 117-117 Configuring the ACS Certificate of CWMP

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the CWMP agent configuration mode.	<b>cwmp agent</b>	Mandatory
Enable a CWMP agent.	<b>enable</b>	Mandatory By default, the CWMP agent is disabled.
Configure the CA certificate path required to connect to the ACS server via HTTPS.	<b>certificate ca</b> <i>ca-path</i>	Mandatory The default path is: <i>/flash/tr069/ca.pem.</i>

### Configure ACS Certificate Fingerprints for CWMP

From security consideration, when the device connects to ACS by HTTPS, it can configure the required certificate fingerprint and verify its validity directly with the fingerprint of the server-side certificate.

Table 31-32 Configuring the ACS Certificate Fingerprint for CWMP

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the CWMP agent configuration mode.	<b>cwmp agent</b>	Mandatory
Enable a CWMP agent.	<b>enable</b>	Mandatory By default, the CWMP agent is disabled.
Configure the certificate fingerprint required to connect to the ACS server via HTTPS.	<b>certificate ca fingerprint</b> <i>fingerprint-string</i>	Mandatory <i>fingerprint-string</i> specifies the fingerprint information to verify the CA certificate, the content is a 40-bit hexadecimal number.

---

### Note

- You can choose one of the two ways to configure the ACS certificate and the ACS certificate fingerprint, and if both are configured, the ACS certificate will be used first.
- 

## 117.8.3 Configure CWMP Extended Functions

### Configuration Condition

Before configuring the extended functionality of CWMP, do the following:

- The basic configuration of CWMP has been completed, including the enabling configuration of the CWMP agent and the information configuration of the ACS proxied by the CWMP agent.
- Layer-3 interface IP addresses have been configured so that neighbor nodes are reachable at the network layer.
- When you need to use the link backup function, the Layer-3 interface configured as backup should be functional, including the IP address configured and the interface

status as UP.

### Configure CWMP to Specify the Source IP Address

With a source IP address configured, the ACS communicates directly with this specified IP address.

Table 33-34 Configuring CWMP to Specify the Source IP Address

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the CWMP agent configuration mode.	<b>cwmp agent</b>	Mandatory
Enable a CWMP agent.	<b>enable</b>	Mandatory By default, the CWMP agent is disabled.
Configure the source IP address specified by the CWMP agent.	<b>ip source <i>ip-address</i></b>	Mandatory By default, the source address of the packet is not specified when the device is building a link with ACS, and the source address of the packet is the output interface of the packet.

### Configure CWMP Link Backup

After the link backup function is configured in the interface mode, it enables the device with multiple WAN ports to be configured, with one default WAN port and the others are backup WAN ports. Generate a connection request URL with the default WAN port IP to send to ACS during normal times. When the default WAN port is down, it will choose one from the backup WAN port as the current WAN port, and then use its IP to generate the connection request URL.

Table 35-36 Configuring CWMP Link Backup

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the Layer-3 interface where backup needs to be set.	<b>interface</b> <i>interface-name</i>	Mandatory
Configure the backup interface proxied by the CWMP agent.	<b>cwmp wan backup</b>	Mandatory By default, no wan device backup interface is specified for the CWMP agent.

## Note

- Only one CWMP wan default interface and one CWMP wan backup interface can be configured per device.

## 117.8.4 CWMP Monitoring and Maintaining

Table 37-38 CWMP Monitoring and Maintaining

Command	Description
<b>show cwmp agent</b>	Display relevant information about the CWMP agent.
<b>show cwmp session</b>	Display information about CWMP agent sessions.
<b>show cwmp methods</b>	Display the RPC (Remote Procedure Call) methods supported by the CWMP agent.
<b>show cwmp parameter all</b>	Display the names of all parameters of the CWMP agent.

Command	Description
<b>show cwmp parameter</b> <i>para-string</i>	Display detailed information of a specified parameter of the CWMP agent.
<b>show cwmp parameter notify</b> { <b>active</b>   <b>all</b>   <b>forceactive</b>   <b>passive</b> }	Display the parameter names of an advertisement of the CWMP agent.
<b>show cwmp parameter values</b> [ <i>para-string</i>   <b>error</b> ]	Display detailed information of a specified parameter of the CWMP agent.

## 117.9 Typical Configuration Example of CWMP

### 117.9.1 Configure the Authentication Function of CWMP

#### Network Requirements

- Device accesses ACS through Network, enables CWMP function on Device, and configures authentication function on both Device and ACS.
- After the authentication succeeds, Device will perform version upgrade, configuration recovery, configuration backup, and configuration upgrade tasks issued by ACS.

#### Network Topology



Figure 117-117 Network Topology for Configuring the CWMP Authentication Function

#### Configuration Steps

- Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)
- Step 2: Configure the IP address and route of the interface. (Omitted)
- Step 3: Configure CWMP.

#Enable the CWMP agent and file download function on Device and configure the URL of ACS.

```
Device#configure terminal
Device(config)#cwmp agent
Device(config-cwmp)#enable
Device(config-cwmp)#management server url http://129.255.136.200:8080/openacs/acs
Device(config-cwmp)#enable download
Device(config-cwmp)#exit
```

#Configure the VLAN2 interface as the default WAN device.

```
Device(config)#interface vlan 2
Device(config-if-vlan2)#cwmp wan default
Device(config-if-vlan2)#exit
```

Step 4: Configure the ACS server.

#Create a fragment template on the ACS and configure both the username and password used for authentication to be admin. (Omitted)

#Create a configuration upgrade task on the ACS, select the created fragment template, and send the configuration upgrade task to Device. (Omitted)

---

## Note

- The ACS ensures that the it can be authenticated by Device by configuring the upgrade task to send the username and password used for authentication down to Device.
- 

#Create version upgrade task/configuration recovery task/configuration backup task on ACS.

Step 5: Check the result.

#The user name and password issued by ACS to Device can be seen on Device via the **show running-config** command.

```
cwmp agent
management server url http://129.255.136.200:8080/openacs/acs
connection request username admin
connection request password admin
enable download
enable
exit
```

#Device can successfully execute the version upgrade task/configuration recovery task/configuration backup task issued by ACS.

## 117.9.2 Configure CWMP to Specify the Source IP Address

### Network Requirements

- Device accesses ACS through Network, enables CWMP function on Device.
- Specify the source IP address of CWMP as 1.0.0.1 to allow Device to access the ACS through the firewall and perform the version upgrade, configuration recovery, and configuration backup tasks issued by the ACS.

### Network Topology

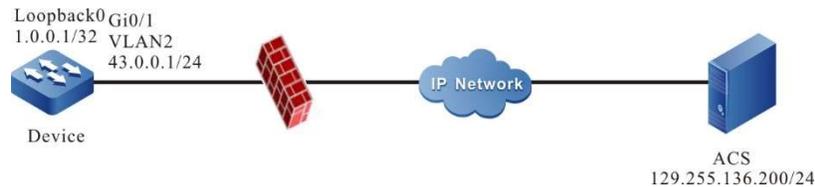


Figure 15-16 Network Topology for Configuring Specified Source IP Address

### Configuration Steps

- Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)
- Step 2: Configure IP addresses and routes for the ports. (Omitted)
- Step 3: Configure CWMP.

#Enable the CWMP agent and file download function on Device, configure the URL of ACS, and configure the source IP address of CWMP as 1.0.0.1.

```
Device#configure terminal
Device(config)#cwmp agent
Device(config-cwmp)#enable
Device(config-cwmp)#management server url http://129.255.136.200:8080/openacs/acs
Device(config-cwmp)#enable download
Device(config-cwmp)#ip source 1.0.0.1
Device(config-cwmp)#exit
```

#Configure the Loopback0 interface as the default WAN device.

```
Device(config)#interface loopback 0
Device(config-if-loopback0)#cwmp wan default
Device(config-if-loopback0)#exit
```

- Step 4: Configure the firewall.

#The firewall denies the passage of packets with the source IP address 43.0.0.1 and allows the passage of packets with the source IP address 1.0.0.1.

- Step 5: Configure the ACS server.

#Create version upgrade task/configuration recovery task/configuration backup task on ACS.

Step 6: Check the result.

#The configured source IP address can be seen on Device by **show running-config**.

```
Device#show running-config
cwmp agent
management server url http://129.255.136.200:8080/openacs/acs
enable download
enable
ip source 1.0.0.1
exit
```

#Device can successfully execute the version upgrade task/configuration recovery task/configuration backup task issued by ACS.

### 117.9.3 Configure CWMP Link Backup

#### Network Requirements

- Device can access the ACS through two lines, giving preference to the VLAN2 interface to communicate with the ACS.
- When the VLAN2 interface fails, Device communicates with the ACS through the VLAN3 interface, and when the VLAN2 interface is restored, Device communicates with the ACS through the VLAN2 interface.

#### Network Topology



Figure 117-117 Network Topology for Configuring CWMP Link Backup

#### Configuration Steps

Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configure IP addresses and routes for the ports. (Omitted)

Step 3: Configure CWMP.

#Enable the CWMP agent and file download function on Device and configure the URL of ACS.

```
Device#configure terminal
Device(config)#cwmp agent
Device(config-cwmp)#enable
Device(config-cwmp)#management server url http://129.255.136.200:8080/openacs/acs
Device(config-cwmp)#enable download
```

```
Device(config-cwmp)#exit
```

#Configure the VLAN2 interface as the default WAN device.

```
Device(config)#interface vlan2
Device(config-if-vlan2)#cwmp wan default
Device(config-if-vlan2)#exit
```

#Configure the VLAN3 interface as the backup WAN device.

```
Device(config)#interface vlan3
Device(config-if-vlan3)#cwmp wan backup
Device(config-if-vlan3)#exit
```

Step 4: Check the result.

#Check the CWMP agent information on Device.

```
Device#show cwmp agent
Agent status: Enabled
Periodic Inform: Enabled
Download files: Enabled
Inform interval: 43200
ACS URL: http://129.255.136.200:8080/openacs/acs
ACS user name:
ACS user password:
Connection request URL: http://42.0.0.1:7547/00017A/HIT SW/00017a136922/cwmp
Connection request user name:
Connection request password:
Default WAN device: vlan2
Current WAN device: vlan2
CA certificate: /flash/tr069/ca.pem
```

It can be seen that the default WAN device is VLAN2 and the current WAN device is VLAN2. It can be seen that the IP address of Device corresponding to 42.0.0.1 in the device management page of ACS.

#Check the CWMP agent information when the VLAN2 interface on Device fails.

```
Device#show cwmp agent
Agent status: Enabled
Periodic Inform: Enabled
Download files: Enabled
Inform interval: 43200
ACS URL: http://129.255.136.200:8080/openacs/acs
ACS user name:
ACS user password:
Connection request URL: http://43.0.0.1:7547/00017A/HIT SW/00017a136922/cwmp
Connection request user name:
Connection request password:
Default WAN device: vlan2
Current WAN device: vlan3
CA certificate: /flash/tr069/ca.pem
```

It is indicated that the default WAN device is VLAN2 and the current WAN device is VLAN3. It can be seen that the IP address of Device corresponding to 43.0.0.1 in the device management page of ACS.

#After the VLAN2 interface on Device is restored, check the CWMP agent information and see that both the default WAN device and the current WAN device are VLAN2. You can see the IP address of Device on the device management page of ACS is 42.0.0.



# 118 NETCONF

---

## 118.1 Overview

NETCONF (Network Configuration Protocol) is an XML-based network management protocol that provides a programmable approach of configuring and managing network devices. Through NETCONF, you can configure device parameters, retrieve parameter values, and get statistics information. All NETCONF packets are XML-based and feature powerful filtering capabilities. Each data item has a fixed element and position. This enables devices of the same vendor to use the same access mode and result display mode. The devices of different vendors can achieve the same effect by XML mapping. This feature facilitates third-party software development and NMS software customization in the multi-vendor, multi-device environment. With the help of such NMS software, NETCONF simplifies device configuration and improves device configuration efficiency.

## 118.2 NETCONF Basic Function Configuration

Table 11- 1 NETCONF Basic Function Configuration Task List

Configuration Task	
NETCONF Server Functions Configuration	Enable the NETCONF Server Function
	NETCONF Client Session Idle Timeout Time Configuration
	Configuring the Maximum Number of NETCONF Sessions
Configuring the functions of NETCONF CALL-HOME	Configuring the functions of NETCONF CALL-HOME

## 118.2.1NETCONF Server Functions Configuration

### Configuration Condition

Before configuring the functions of NETCONF server, ensure that:

- The link layer protocol has been configured to ensure normal communication at the link layer.
- Interface network layer addresses have been configured so that NETCONF client nodes are reachable at the network layer.

### Enable the NETCONF Server Function

Table 11- 2 Enabling NETCONF Server Task List

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable the Global NETCONF Function	<b>netconf server enable</b>	Mandatory By default, the NETCONF function is disabled

### NETCONF Client Session Idle Timeout Time Configuration

Table 11- 3 NETCONF Client Session Idle Timeout Time Configuration

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable the Global NETCONF Function	<b>netconf client idle-time</b>	Mandatory By default, the NETCONF client session idle timeout time is 3600 seconds

### Function of Configuring the Maximum Number of NETCONF Sessions

Table 11- 4 Function of configuring the maximum number of NETCONF sessions

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Function of configuring the maximum number of NETCONF sessions	<b>netconf server max-session</b> <i>session-num</i>	Optional By default, the maximum number of sessions supported by NETCONF is 4

## 118.2.2 Configuring the Functions of NETCONF CALL-HOME

### Configuration Condition

Before configuring the functions of NETCONF server, ensure that:

- The link layer protocol has been configured to ensure normal communication at the link layer.
- Interface network layer addresses have been configured so that NETCONF client nodes are reachable at the network layer.

### Configuring the Functions of NETCONF CALL-HOME

The configured CALL-HOME terminal can automatically connect to the configured terminal after the NETCONF service is enabled, thus establishing a NETCONF SSH connection without the client actively connecting to the NETCONF server.

Table 11- 5 NETCONF CALL-HOME Function Configuration

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configuring the functions of NETCONF CALL-HOME	<b>netconf call-home client</b> <i>client-name ssh endpoint-name address host-name</i> <b>[ port port-num ]</b>	Mandatory By default, there is no call-home client

## 118.2.3 NETCONF Monitoring and Maintaining

Table 11- 6 NETCONF Monitoring and Maintaining

Command	Description
<b>debug netconf [ all   cmf   conf   database   dbm   plugin   server   ssh   yang ]</b>	Open NETCONF debugging switch
<b>show netconf session</b>	Display the current NETCONF client connection session information

## 118.3 NETCONF Typical Configuration Example

### 118.3.1 Configure the NETCONF server

#### Network Requirements

- Device1 and Device2 are NETCONF server devices, which are routed through the unicast routing protocol to the controller.
- The controller monitors and manages Device1 and Device2 via NETCONF.

#### Network Topology

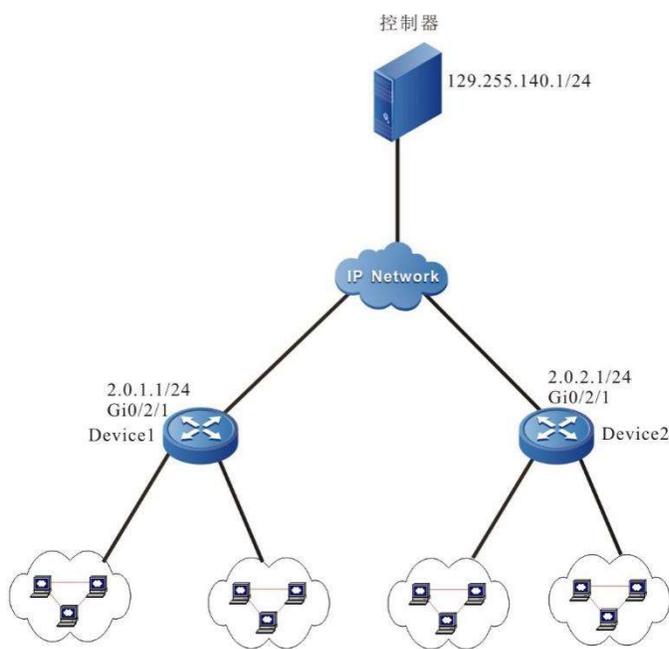


Figure 11- 1 Networking for Configuring the NETCONF Server

## Configuration Steps

A NETCONF connection is established between the configuration controller and the device, and then the controller configures and manages the device via NETCONF. The configuration of Device2 is similar to that of Device1, which shall not be repeated here.

Step 1: Configure IP addresses for the ports. (Omitted)

Step 2: Configure NETCONF users

#Create netconf users on the device with the username "admin" and password "admin@123".

```
Device1#configure terminal
Device1(config)#local-user admin class manager
Device1(config-user-manager-admin)#service-type netconf ftp
Device1(config-user-manager-admin)#password 0 admin@123
Device1(config-user-manager-admin)#privilege 15
Device1(config-user-manager-admin)#exit
```

Step 3: Configure the device to enable the NETCONF server functions.

#Configure the NETCONF server enabling function on the device.

```
Device1(config)#netconf server enable
```

Step 4: Configure the controller.

#Open the controller, click on "Network Planning", select "Network Discovery", click on "New", and configure the NETCONF parameters: "IP Address", "Name", "Account" and "Password". "IP address", where the parameters on "name", "account" and "password" must be configured the same as those on the device. Click OK to establish normal communication between the device and the controller.

**New**
✕

**Central Node 1**
**Central Node 2**

\* **IP Address**

\* **Name**

\* **Account**   
NETCONF Connection Account

\* **Password**   
NETCONF Connection Password

**Description**

Cancel

OK

Step 5: Check the results.

#Connections established between the device query controller and the device NETCONF server.

```

Device1#show netconf session
-----
session id: 1
transport: SSH
user name: admin
source host: 129.255.140.1
login time: 2019-06-1T20:29:05Z
in rpcs: 1
in bad rpcs: 0
out rpc errors: 0
out notifications: 0

```

# 119 Telemetry

---

## 119.1 Overview

Telemetry is a technology that remotely collects data from network devices at high speed. It adopts the Push Mode to obtain rich monitoring data on the network device in a timely manner, so that it can quickly achieve network fault location and efficient and intelligent network operation and maintaining.

With the growing size of the network, traditional network monitoring methods (such as SNMP and CLI) are becoming less and less efficient and can no longer meet the needs of high-performance network monitoring. With the emergence of Telemetry technology, it is able to achieve higher accuracy and more real-time monitoring data collection for super large-scale networks, as well as rapid positioning and resolution of network problems, making it an important big data platform for network quality tuning and providing strong support for the requirements and development of intelligent network operation and maintaining in the future.

The Telemetry function consists of two main parts:

- **Static Subscription**  
Telemetry static subscription means that the device acts as the client, the collector acts as the server, and the device initiates the connection to the collector for data collection and uploading.
- **Dynamic Subscription**  
Telemetry dynamic subscription means that the device acts as the server and the collector acts as the client to initiate the connection to the device, and the device does the data collection and uploading.

## 119.2 Telemetry Function Configuration

Table 119-1 Telemetry Function Configuration List

Configuration Task	
	Configure sensors.

Configuration Task	
Configure Telemetry static subscriptions.	Configure collectors.
	Configure subscriptions.
	Enable subscriptions.
Configuring Telemetry dynamic subscriptions.	Configurd the GRPC server.

## 119.2.1 Configure Telemetry Static Subscriptions

### Configuration Condition

None

### Configure Sensors

When users configure Telemetry static subscription sampling data, they need to create a sampling sensor group, then specify the sampling path information, and configure the required sampling path for the sensor according to the specified sampling path information.

Table 119-2 Configuring Sensors

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the sensor group mode.	<b>telemetry sensor-group</b> <i>sensor-name</i>	Mandatory If this group does not exist, it is created directly before entering the group mode, otherwise it enters the group module directly.
Configure sensor paths.	<b>sensor-path</b> <i>path-name</i>	Mandatory

## Configuring Target Collectors

When users configure Telemetry to statically subscribe to sample data, they need to create the upload target group and then specify target collectors to which the sample data is to be uploaded.

Table 119-119 Configuring Target Collectors

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the sensor group mode.	<b>telemetry destination-group</b> <i>destination-name</i>	Mandatory If the group exists, it will go directly into the group mode.
Configure the destination address.	<b>ipv4-address [vrf vrf-name] ip-address port</b> <i>port-num</i>	Mandatory Vrf uses global by default. The port takes values in the range of 1 to 65535.

## Creating the Subscription

When users configure Telemetry to statically subscribe to sampling data, they need to create a subscription, associate the configured upload target group with the sampling sensor group, and finish uploading data after enabling.

Table 119-119 Creating Subscriptions

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Enter the subscription group mode,	<b>telemetry subscription</b> <i>subscription-name</i>	Mandatory
Configure the source interface that sends subscriptions.	<b>source-interface</b> <i>interface-name</i>	Optional By default, the output interface will be determined based on the route and the primary IP address of the output interface will be used as the source IP address for sending
Configure associated sensor groups.	<b>sensor-group</b> <i>sensor-name</i> [ <b>sample-interval</b> <i>sample-interval</i> ]	Mandatory If the sensor group does not exist, you need to configure the sensor group first.  The default value of sample-interval is 10000 milliseconds.
Configure the associated uploading destination group.	<b>destination-group</b> <i>destination-name</i>	Mandatory If the target group does not exist, you need to configure the uploading target group first.
Configure to enable subscriptions.	<b>subscription enable</b>	Mandatory Complete data upload after being enabled.

## 119.2.2 Configuring Telemetry Dynamic Subscriptions

### Configuration Condition

User manual  
Release 1.0 01/2022

None

### Enable GRPC Server

Dynamic subscription is when the device side is acting as the server, therefore, the GRPC server function of the device should be enabled, if you need to complete the dynamic subscription data upload, you need the collector to act as the client, and connect it to the the device side.

Table 119-119 Configuring GRPC Servers

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable GRPC Server	<b>grpc server [port <i>port-num</i>]</b>	Mandatory The default value of the <b>port</b> is 51700.

### 119.2.3 Telemetry Monitoring and Maintaining

Table 3-4 Telemetry Monitoring and Maintaining

Command	Description
<b>show telemetry sensor-group</b> [ <i>sensor-name</i> ]	View the sampling sensor information, the display includes the configured sampling path information.
<b>show telemetry destination</b> [ <i>destination-name</i> ]	View the uploading destination group information, including the configured uploading destination address information.
<b>show telemetry subscription</b> [ <i>subscription-name</i> ]	View subscription information, displaying information about the configured associated sensor group and target group.

Command	Description
<b>show telemetry sensor-path</b>	View Telemetry sensor sample paths, display includes information on supported sample paths.
<b>show telemetry dynamic-subscription</b> [ <i>dynamic-subscription-name</i> ]	View Telemetry dynamic subscription statistics, displaying information including dynamically subscribed sensor path information.

## 119.3 Typical Configuration Example of Telemetry

### 119.3.1 Configure Telemetry Static Subscriptions

#### Network Requirements

- Device acts as a Telemetry client and actively sends data to the server.
- The Telemetry service is enabled on the server and actively listens on port 30000.

#### Network Topology

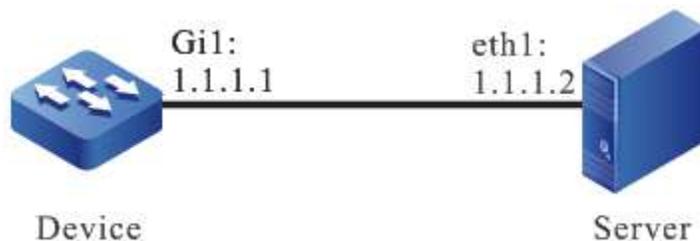


Figure 4- 1 Network Topology for Static Subscription

#### Configuration Steps

- Step 1: Enable Telemetry service on server and configure to listen on port 30000, omitted.
- Step 2: Configure the static subscription function Telemetry.

#Create a sample group sensor and configure the sample path as dmm/memInfo, which is used to count memory usage and other situation data.

```
Device#configure terminal
Device(config)#telemetry sensor-group sensor
Device(config-telemetry-sensor-group-sensor)#sensor-path dmm/memInfo
Device(config-telemetry-sensor-group-sensor)#exit
```

#Create a target group, configure the target address to be the address of the server, and configure the port to be the port the server is listening on.

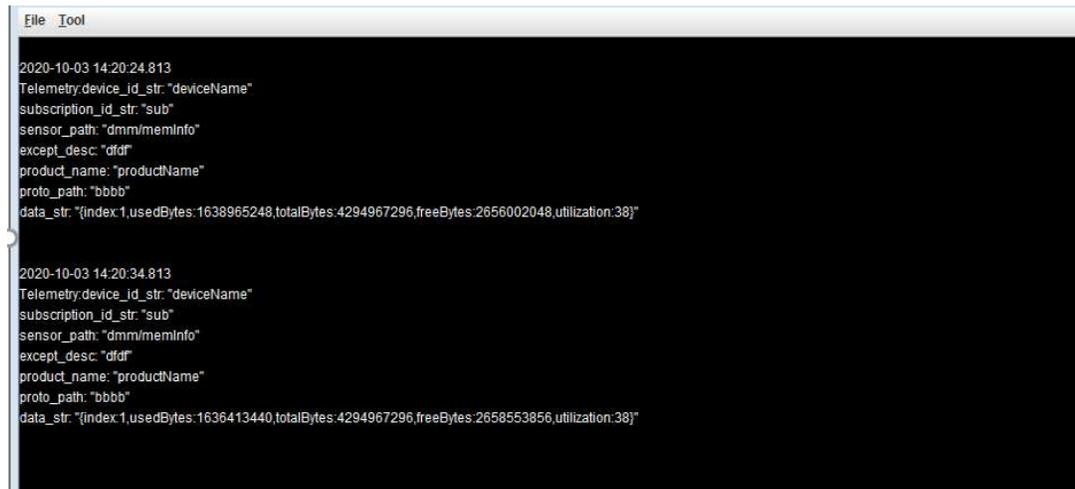
```
Device(config)#telemetry destination-group dest
Device(config-telemetry-destination-group-dest)#ipv4-address 1.1.1.2 port 30000
Device(config-telemetry-destination-group-dest)#exit
```

#Configure the subscription group, refer to the sensor combination target group configured above, and enable the subscription function.

```
Device(config)#telemetry subscription sub
Device(config-telemetry-subscription-sub)#sensor-group sensor sample-interval 10000
Device(config-telemetry-subscription-sub)#destination-group dest
Device(config-telemetry-subscription-sub)#subscription enable
```

Step 3: Check the result.

#The device can receive memory statistics via Telemetry every 10s on the collector.



```
File  Tool
2020-10-03 14:20:24.813
Telemetry.device_id_str:"deviceName"
subscription_id_str:"sub"
sensor_path:"dmm/memInfo"
except_desc:"dfd"
product_name:"productName"
proto_path:"bbb"
data_str:"{index:1,usedBytes:1638965248,totalBytes:4294967296,freeBytes:2656002048,utilization:38}"

2020-10-03 14:20:34.813
Telemetry.device_id_str:"deviceName"
subscription_id_str:"sub"
sensor_path:"dmm/memInfo"
except_desc:"dfd"
product_name:"productName"
proto_path:"bbb"
data_str:"{index:1,usedBytes:1636413440,totalBytes:4294967296,freeBytes:2658553856,utilization:38}"
```

Figure 119-2 Memory Usage Statistics Received by the Collector

## 119.3.2 Configuring Telemetry Dynamic Subscriptions

### Network Requirements

- Client acts as a Telemetry client and is used to send Telemetry data requests to the device and display the data replied by the device.
- Device acts as the Telemetry server to respond to requests from the device.

## Network Topology

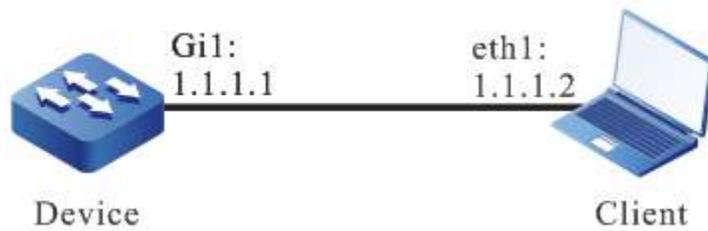


Figure 119-3 Network Topology for Dynamic Subscription

## Configuration Steps

Step 1: Enable GRPC service on the device.

```
Device#configure terminal
Device(config)#grpc server
```

Step 2: The Telemetry data request is placed on the client, omitted.

Step 3: Check the result.

#Show on the device to see dynamic subscription connections.

```
Device#show telemetry dynamic-subscription

1.Telemetry dynamic-subscription Information:
-----
Subscription-name   : dynSubs96183
Subscription-id     : 96183
Request-id          : 3874318141
Encoding            : JSON
Sample-interval(ms): : 10000
Subscription-state  : Subscribed
-----
Sensor group information:
-----
Sample-interval(ms)  Sample-path
-----
10000                dmm/memInfo
-----
```

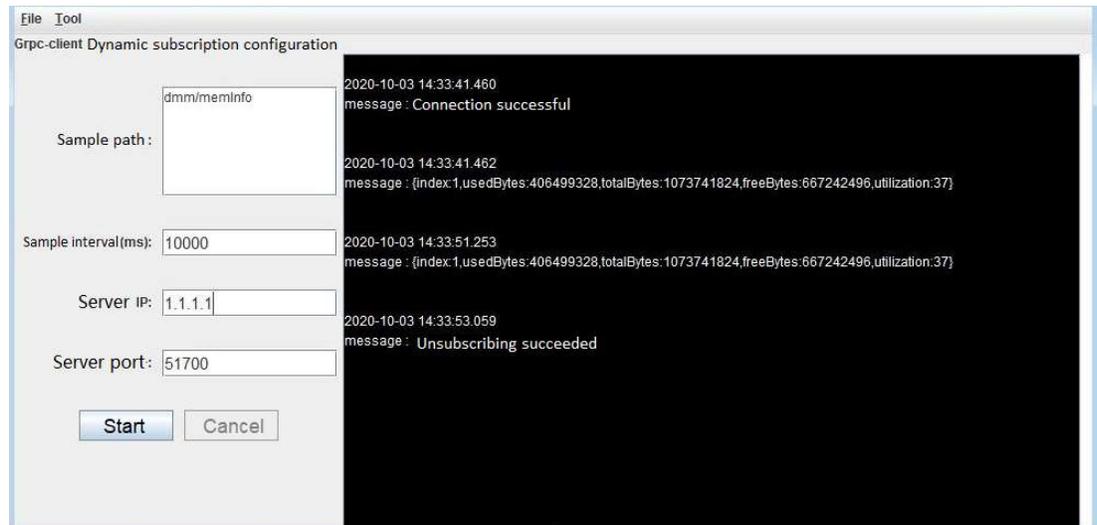


Figure 1-2 Information on Data Transmission of Clients

# 120 sFlow

---

## 120.1 Overview

sFlow, a technology for network traffic sampling and monitoring, follows the RFC3176 standard. sFlow performs different samplings according to different configurations. The sampling process is: First analyze the packet head from the sampled packet, encapsulate as the sFlow packet according to the standard definition, and send to the third-party receiver, which is convenient for the user to analyze and monitor the traffic entering the device via the third-party receiver.

sFlow includes the following two sampling modes:

- Sampler sampling mode: It is one sampling mode provided by the switching chip, sampling the traffic entering the port at random;

- Poller sampling mode: It is one software sampling mode, used to collect the packet and traffic statistics information of the port regularly.

sFlow defines the following two roles:

- Agent role: It is the sFlow agent on the device, used to manage the two sampling modes of sFlow and execute the sampling task;
- Receiver role: It is the mapping of the third-party receiver supporting the sFlow protocol on the local device, used to save the information of the third-party receiver (such as IP address and UDP port number) and regularly send the sFlow packets buffered on the device to the third-party receiver.

## 120.2 sFlow Function Configuration

Table 120-120 sFlow Function Configuration List

Configuration Task	
Configure basic functions of sFlow.	Create the agent role.
	Create receiver Role
Configure sFlow Sampling Mode	Configure sampler Sampling Mode
	Configure poller Sampling Mode

### 120.2.1 Configure Basic Functions of sFlow

#### Configuration Condition

- No.

#### Create the Agent Role

The agent role is used to configure and manage sampling. Currently, the network address type supported by the agent role can only be IPv4.

Table 120-120 Creating the Agent Role

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Create the agent role.	<b>sflow agent ip</b> <i>ip-address</i>	Mandatory By default, no agent role is created.

### Create Receiver Role

The receiver role is used to save the information of the third-party receiver and send the sFlow packets buffered on the device to the third-party receiver via the UDP mode. The triggering conditions of sending packets include the following two:

- When the specified buffer area is full and cannot be filled with new sFlow sampling information, first encapsulate the buffered part to the sFlow packet, send to the third-party receiver, and then fill the new part to the buffer area. This can reduce the number of the sFlow packets sent by the device to the third-party receiver obviously.
- Encapsulate the buffered sFlow sampling information as the sFlow packet periodically and send to the third-party receiver. This can avoid that the buffered part cannot be encapsulated as the sFlow packet and sent to the third-party receiver because of not receiving new sFlow sampling information within a long time.

Table 120-120 Creating the Receiver Role

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Create receiver Role	<b>sflow receiver</b> <i>receiver-index</i> <b>owner</b> <i>owner-name</i> <b>ip</b> <i>ip-address</i> [ <b>packet-size</b> <i>packet-size-value</i> <b>timeout</b> <i>timeout-value</i> <b>udp-port</b> <i>udp-port-number</i> ]	Mandatory By default, no receiver role is created.

## 120.2.2 Configure sFlow Sampling Mode

### Configuration Condition

Before configuring the sFlow sampling mode, first complete the following task:

- Create the agent role
- Create the receiver role

### Configure Sampler Sampling Mode

In the sampler sampling mode, that is port flow sampling, the switching chip samples the traffic received by the port at random. After getting the sample packet, first copy the head information of the packet, resolve the copied content, get the desired sample information from it, and at last, encapsulate the sample information and send to the corresponding third-party receiver of the receiver role.

Table 120-120 Configuring the Interface Sampler Sampling Method

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	-
Configure sampler Sampling Mode	<b>sflow sampler receiver</b> <i>receiver-index</i> [ <b>header-size</b> <i>header-size-value</i> <b>sample-rate</b> <i>sample-rate-value</i> <b>direction</b> <i>direction-value</i> <b>type</b> <i>type-value</i> ]	Mandatory  By default, do not configure the sampler sampling mode.

### Configure Poller Sampling Mode

The poller sampling mode, that is port regular polling sampling, is to regularly encapsulate the packet and traffic statistics information on the port within the period and send to the corresponding third-party receiver of the receiver role.

Table 1-2 Configuring the Poller Sampling Method

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	-
Configure poller Sampling Mode	<b>sflow poller</b> <i>poller-index</i> <b>receiver</b> <i>receiver-index</i> [ <b>interval</b> <i>interval-value</i> <b>type</b> <i>type-value</i> ]	Mandatory  By default, no poller sampling method is configured.

### 120.2.3sFlow Monitoring and Maintaining

Table 120-120 sFlow Monitoring and Maintaining

Command	Description
<b>clear sflow receiver</b> <i>receiver-index</i> <b>statistics</b>	Clear the sFlow sampling statistics associated with the specified receiver role.
<b>show sflow</b>	Display the configuration and operation information of sFlow.
<b>show sflow agent</b>	Display the configuration and operation information of the agent role.
<b>show sflow poller</b> [ <b>interface</b> <i>interface-name</i> ]	Display the configuration and operation information of the poller sampling method on the interface.
<b>show sflow receiver</b> [ <i>receiver-index</i> [ <b>statistics</b> ] ]	Displays sFlow sampling statistics, configuration and operational information associated with the receiver role.

Command	Description
<b>show sflow sampler</b> [ <b>interface interface-name</b> ]	Display the configuration and operation information of the sampler sampling method on the interface.

## 120.3 Typical Configuration Example of sFlow

### 120.3.1 Configure Basic Functions of sFlow

#### Network Requirements

- Device is an sFlow agent device that is route reachable to the NMS server.
- The NMS server monitors Device's interface data traffic via sFlow.

#### Network Topology



Figure 120-120 Network Topology for Configuring Basic Functions of sFlow

#### Configuration Steps

- Step 1: Configure the VLAN and add the interface to the corresponding VLAN. (Omitted)
- Step 2: Configures IP addresses for the ports. (Omitted)
- Step 3: Configure the sFlow function.

#### #Enable an sFlow agent.

```
Device#configure terminal
Device(config)#sflow agent ip 1.1.1.1
```

#Configure the destination IP address and destination UDP interface number of the sFlow statistics output packet, the sending interval of packets is 5 seconds, and the cache is 1400 bytes.

```
Device(config)#sflow receiver 1 owner 1 ip 129.255.151.10 timeout 5 udp-port 6343 packet-size 1400
```

#Sampler sampling of the flow in the inbound direction of interface gigabitethernet0/1 with a sampling frequency of 10.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#sflow sampler receiver 1 sample-rate 10 direction rx
```

#Poller sampling of flows in the inbound direction of interface gigabitethernet0/1 with a polling period of 20 seconds.

```
Device(config-if-gigabitethernet0/1)#sflow poller 1 receiver 1 interval 20
Device(config-if-gigabitethernet0/1)#exit
```

Step 4: Check the result.

#View information about the sFlow on Device.

```
Device#show sflow
```

sFlow Agent Configuration: (Interval = 120, Current Tick = 0x002a6476)

Version	Id	Type	Net Address	Receivers Socket	Samplers Number	Pollers Number	Number	Boot Time / Exec Time
1.3	1	IPv4	1.1.1.1	0x1c 1/10	1/864	1/864	0x00000ab2/0x002a644c	

sFlow Receivers Configuration: (Reset Delta = 18000, Current Tick = 0x002a6476)

sFlow Receivers num:1(limit 10)

Index	Owner	Net Address	Port	Version	Datagram	Timeout	Reset Time	Expire Time
1	1	129.255.151.10	6343	5	1400	5	0x002a644c/0x002a6578	

sFlow Samplers Configuration:

sFlow Samplers num:1(limit 864)

Sampling Types: H - raw packet header E - ethernet packet  
F - IPv4 packet S - IPv6 packet

Interface	Index	Rate	Direction	Header	Types
gi0/1	1	10	rx	128	H

sFlow Pollers Configuration: (Current Tick = 0x002a6476)

sFlow Pollers num:1(limit 864)

Sampling Types: G - generic counter  
E - ethernet counter

Receiver Sampling				
Interface	Instance	Index	Types	Interval
gi0/1	1	1	G	20

#The flow information of the inbound direction of interface gigabitethernet0/1 on Device can be viewed on the NMS.

# 121 VST

---

## 121.1 Overview

With the ever-increasing requirements of users for reducing costs and improving equipment reliability, we have proposed a technology that combines multiple physical switches into one virtual switch, namely Virtual Switching Technology (VST).

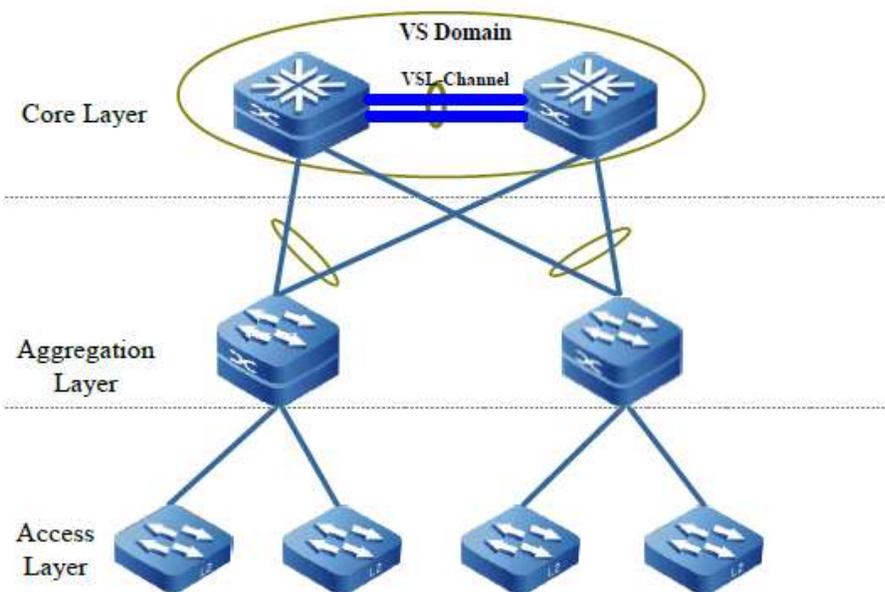


Figure 121-1 VST Physical Network View

As shown in Figure 1-1, two devices at the core layer are connected via a virtual switching link interface to form one VS Domain (virtual switching domain, also called stack system); the devices at the aggregation layer are uplinked to VS Domain via link aggregation; the VS Domain at the core layer is one virtual device to other network devices.

Compared with the traditional L2 spanning tree and L3 VRRP/VBRP technology, this technology has the following advantages:

- Exponential Increase in Bandwidth under Efficient Use

In the traditional solution, due to the operation of STP/RSTP/MSTP, one of the original two uplinks will be in the forwarding status and the other link in the backup status; multiple devices become one single logical device by the use of the virtual switching technology, and therefore, it is no longer necessary to block some links; two links form one aggregation group, which can be used to forward data, thereby effectively using the bandwidth of these links without causing the waste of bandwidth resources. In addition, the cross-device and cross-board aggregation link allow for both redundant links and dynamic load balancing, thereby effectively utilizing all bandwidth.

- High reliability

Virtual switching system is composed of multiple member devices. The master control device is responsible for the operation, management, and maintenance of the entire virtual switching system, while other member devices are in the backup status. Once the master control device fails, there will be no rely on the convergence of STP/RSTP/MSTP, VRRP/VBRP and other protocols, and the system will quickly elect the new master control device from other member devices in the backup status, ensuring

that the business of the virtual switching system experiences no interruption, and improved reliability is provided when member failure occurs.

- **Network Topology Simplification**

The virtual device formed by means of the virtual switching technology is equivalent to a single device in the network. It is connected to the peripheral devices via aggregation links. Because there is no L2 loop, there is no need to configure the STP/RSTP/MSTP protocol. Various control layer protocols run on one virtual device, thereby reducing the interaction of numerous protocol packets between the devices and shortening the routing convergence time.

- **Centralized Management**

After two or more devices form stack system, the member device control plane in the virtual switching system is in the backup status, but its data plane is active. Users can log in to the virtual switching system via the port of any member device to carry out centralized management on the entire virtual device, without connecting to each member device for separate management.

## **121.1.1 Basic Concepts**

### **Virtual Switch Domain**

Virtual switch domain is composed of one or more member devices. The member devices in the same virtual switch domain must have the same domain ID configuration. The domain ID uniquely determines one virtual switch domain. When the virtual switch domain MAC address is obtained using the virtual MAC address mode, the virtual switch domain ID uniquely determines the MAC address. Therefore, in the same LAN, the domain IDs between multiple stack systems cannot be the same.

### **Virtual Switch Member Device**

Each physical device in the virtual switch domain is also called virtual switch member device. In the same stack domain, the member ID uniquely determines one member device.

### **Virtual Switch Link Interface and its Member Port**

By binding the multiple physical ports together which are stacking capable, one virtual switch link interface (VSL-Channel) can be formed. The virtual switch link interface is logical link channel for internal protocol packet interaction and service data forwarding between member devices in the stack system, and each physical port therein is called virtual switch link member port.

The member devices join the same virtual switch domain, interconnect with each other via the virtual switch link interface, and finally form one virtual switch device.

### **LMP**

LMP (Link Manage Protocol) is used to manage the virtual switch link interface and its member ports.

## RRP

RRP (Role Resolution Protocol) is used for the role resolution of member devices in the stack system.

## TDP

TDP (Topology Discovery Protocol) is used to advertise the information of the member devices in the stack system to ensure information consistency for all member devices in the stack system.

## 121.2 VST Function Configuration

Table 121-1 VST Function Configuration List

Configuration Task	
Configure virtual switch member device	Configure virtual switch member device domain ID
	Configure virtual switch member device ID
	Configure virtual switch member device priority
Configure virtual switch link interface	Create virtual switch link interface
	Configure to add the port to the virtual switch link interface
Configure device running mode	Configure device running mode
Configure the maximum number of devices supported by the stack system	Configure the maximum number of devices supported by the stack system

## 121.2.1 Configure Virtual Switch Member Device

Before the device joins the virtual switch stack domain or after it has joined the virtual switch stack domain, you can configure the device accordingly, including modifying its member ID, domain ID, and priority.

---

### Note

- In the stack mode, after modifying the member ID or domain ID of the virtual switch member device, the newly configured member ID or domain ID will not take effect immediately. The corresponding configuration will only take effect after the corresponding virtual switch member device saves the configuration and reboots.
- 

### Configuration Condition

None

### Configure Virtual Switch Member Device Domain ID

Table 121-2 Configuring Virtual Switch Member Device Domain ID

Step	Command	Description
Enter the virtual switch member configuration mode	<b>switch virtual member</b> <i>member-id</i>	-
Configure virtual switch member device domain ID	<b>domain</b> <i>domain-id</i>	Mandatory  By default, the domain ID of the virtual switch member device is 100

---

### Caution

- In the stack mode, when adding a virtual switch member device to the virtual switch domain, you must ensure that the domain ID of every virtual switch member device is the same, otherwise the virtual switch member device will not be able to join the same virtual switch domain.
-

- 
- In the stack mode, after the domain ID is modified, the new domain ID will not take effect immediately. The new domain ID will only take effect after the virtual switch member device saves the configuration and reboots.
- 

### Configure Virtual Switch Member Device ID

For configuring the virtual switch member device ID, there are two corresponding cases: In the first case, the device has never been configured with the virtual switch member device ID and requires a virtual switch member device ID to be configured; In the second case, the device has been configured with a virtual switch member device ID and requires it to be modified into the new virtual switch member device ID. Therefore, there are two commands to configure the virtual switch member device ID. One is to configure the virtual switch member device ID, and the other is to modify the virtual switch member device ID, as shown in Table 1-3.

Table 121-3 Configuring VST Member Device ID

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure virtual switch member device ID	<b>switch virtual member</b> <i>member-id</i>	Mandatory By default, the device has no virtual switch member device ID
Modify virtual switch member device ID	<b>switch virtual member</b> <i>member-id rename</i> <i>member-id-new</i>	Optional

---

### Caution

- In the stack mode, after modifying the virtual switch member device ID, you must save the configuration and reboot the system before the new virtual switch member device ID takes effect.
  - In the stack mode, after modifying the virtual switch member device ID, you must save the configuration and reboot the system before the new virtual switch member device ID takes effect. In one virtual switch domain, the member ID of each virtual switch member device is unique, and it cannot happen that the member IDs of two virtual switch member devices are the
-

---

same, otherwise the virtual switch member devices cannot be stacked normally.

---

### Configure Virtual Switch Member Device Priority

When multiple virtual switch member devices join the same virtual switch domain, the priority of each virtual switch member device can be configured to increase the possibility of the virtual switch member device being selected as the master control device. The higher the priority value, the more preferred.

Table 121-4 Configuring Virtual Switch Member Device Priority

Step	Command	Description
Enter the virtual switch member configuration mode	<b>switch virtual member</b> <i>member-id</i>	-
Configure virtual switch member device priority	<b>priority</b> <i>priority-num</i>	Mandatory  By default, the priority of the virtual switch member device is 100

---

### Note

- The virtual switch master control devices in the virtual switch domain are selected based on the following resolution rules:
    1. The virtual switch master control device is given priority; if there are multiple virtual switch master control devices, the second step comparison is performed; if there is no virtual switch master control device, the third step comparison is performed, otherwise the comparison ends;
    2. Those as the virtual switch master control device having a long run time are given priority; if the master control devices have the same run time, the third step comparison is performed, otherwise the comparison ends;
    3. Those higher priority are given priority; if the priorities are the same, the fourth step comparison is performed, otherwise the comparison ends;
    4. Those having small member ID are given priority.
-

## 121.2.2 Configure Virtual Switch Link Interface

The virtual switch link interface (VSL-Channel) is one logical interface. Centralized management for multiple physical ports is achieved by binding together these physical ports that support stacking. Any operation on the virtual switch link interface will affect every physical member port at the same time.

### Configuration Condition

None

### Create Virtual Switch Link Interface

Table 121-5 Creating Virtual Switch Link Interface

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Create virtual switch link interface	<b>vsl-channel</b> <i>vsl-channel-id</i>	Mandatory  In stand-alone mode, vsl-channel-id is a one-dimensional value that represents a virtual switch link interface ID. In the stack mode, it is a two-dimensional value. The first dimension is a virtual switch member ID, and the second dimension is a virtual switch link interface ID.

---

### Caution

- Upon deletion of the virtual switch link interface, all member ports in the virtual switch link interface will exit the virtual switch link interface, and all the member ports' configurations are restored to the default status. Before deleting the virtual switch link

---

interface, please confirm that there will be no loops in the network after deletion.

---

### Configure to Add the Port to the Virtual Switch Link Interface

Table 121-6 Configuring to Add the Port to the Virtual Switch Link Interface

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	-
Configure to add the port to the virtual switch link interface	<b>vsl-channel</b> <i>vsl-channel-id</i> <b>mode on [ type extern ]</b>	Mandatory

---

#### Note

- All member ports in the virtual switch link interface must have the same port capability level.
- 

### 121.2.3 Configure Device Running Mode

The current device supports two running modes, that is, stand-alone mode and stack mode. The device can form one virtual switch domain with other virtual switch member devices only when it runs in the stack mode.

#### Configuration Condition

None

#### Configure Device Running Mode

Table 121-7 Configuring Device Running Mode

Step	Command	Description
Enter the privileged user mode.	<b>enable</b>	-
Configure device running mode	<b>switch mode { stand-alone   virtual }</b>	Mandatory By default, the device runs in the stand-alone mode

### Note

- When the running mode of the device changes, the device will reboot and run in the new configuration mode after the reboot.
- The different running modes of the device correspond to their respective independent boot configuration files.
- Before switching the device to run in the stack mode, you must ensure that the virtual switch member device ID has been configured, otherwise switching cannot be performed.

## 121.2.4 Configure the Maximum Number of Devices Supported by the Stack System

One stack system is composed of multiple devices. The number of devices that constitute the stack system is limited. The defined limit value is the maximum number of devices supported by the stack system.

### Configuration Condition

None

### Configure the Maximum Number of Devices Supported by the Stack System

Table 121-8 Configuring the Maximum Number of Devices Supported by the Stack System

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Configure the maximum number of devices supported by the stack system	<b>switch virtual max-number</b> <i>number</i>	Mandatory By default, the maximum number of devices supported by the stack system is 2

### Note

- The modification to the maximum number of devices supported by the stack system takes effect only after you save the configuration and reboot the system.

## 121.2.5VST Monitoring and Maintaining

Table 121-9 VST Monitoring and Maintaining

Command	Description
<b>show switch virtual</b>	Show the basic information of the virtual switch domain
<b>show switch virtual local config</b>	Show the basic configuration information of the local virtual switch member device
<b>show switch virtual local current</b>	Show the basic running information of the local virtual switch member device
<b>show switch virtual member</b> <i>member-id</i> [ <b>config</b>   <b>current</b> ]	Show the basic information of the virtual switch member device
<b>show switch virtual topo</b>	Show the information about the forwarding path from the local virtual switch member device to other virtual switch member

Command	Description
	devices in the virtual switch domain
<b>show switch vsl-channel</b> [ <i>vsl-channel-id</i> ]	Show the information about the virtual switch link interface in the virtual switch domain

## 121.3 VST Typical Configuration Example

### 121.3.1 Configure the Devices to Form Chain Stack System

#### Network Requirements

- It is realized that Device0 and Device1 form chain stack system, in which Device0 becomes the master control device.

#### Network Topology

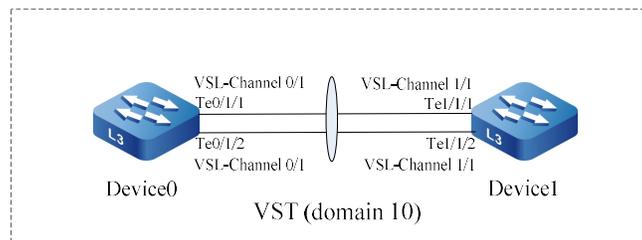


Figure 121-2 Configuring the Devices to Form Chain Stack System

#### Configuration Steps

Step 1: Configure Device0.

#On Device0, Configure the virtual switch member device ID as 0, and configure the domain ID as 10 and the priority as 255.

Device0#configure terminal

```
Device0(config)#switch virtual member 0
Do you want to modify member id(Yes|No)?y
% Member ID 0 config will take effect only after the exec command 'switch mode virtual' is issued
Device0(config-vst-member-0)#domain 10
% Domain ID 10 config will take effect only after the exec command 'switch mode virtual' is issued
Device0(config-vst-member-0)#priority 255
Device0(config-vst-member-0)#exit
```

**#On Device0, create virtual switch link interface 1, and add ports tengigabitethernet1/1 and tengigabitethernet1/2 to the virtual switch link interface 1.**

```
Device0(config)#vsl-channel 1
Device0(config-vsl-channel-1)#exit
Device0(config)#interface tengigabitethernet 1/1-1/2
Device0(config-if-range)#vsl-channel 1 mode on
Device0(config-if-range)#exit
```

**#Save the configuration on Device0.**

```
Device0#write
Are you sure to overwrite /flash/startup (Yes|No)?y
Building Configuration...done
Write to startup file ... OK
Write to mode file... OK
```

## Step 2: Configure Device1.

**#On Device1, Configure the virtual switch member device ID as 1, and configure the domain ID as 10 and the priority as 200.**

```
Device1#configure terminal
Device1(config)#switch virtual member 1
Do you want to modify member id(Yes|No)?y
% Member ID 1 config will take effect only after the exec command 'switch mode virtual' is issued
Device1(config-vst-member-1)#domain 10
% Domain ID 10 config will take effect only after the exec command 'switch mode virtual' is issued
Device1(config-vst-member-1)#priority 200
Device1(config-vst-member-1)#exit
```

**#On Device1, create virtual switch link interface 1, and add ports tengigabitethernet1/1 and tengigabitethernet1/2 to the virtual switch link interface 1.**

```
Device1(config)#vsl-channel 1
Device1(config-vsl-channel-1)#exit
Device1(config)#interface tengigabitethernet 1/1-1/2
Device1(config-if-range)#vsl-channel 1 mode on
```

```
Device1(config-if-range)#exit
```

**#Save the configuration on Device1.**

```
Device1#write
```

```
Are you sure to overwrite /flash/startup (Yes|No)?y
```

```
Building Configuration...done
```

```
Write to startup file ... OK
```

```
Write to mode file... OK
```

**Step 3: Configure Device0 and Device1 to run in the stack mode.**

**#Configure Device0 to run in the stack mode.**

```
Device0#switch mode virtual
```

```
This command will convert all interface names to naming convention "interface-type member-number/slot/interface" ,
```

```
Please make sure to save current configuration.Do you want to proceed? (yes|no)?y
```

```
Converting interface names Building configuration...
```

```
Copying the startup configuration to backup file named "startup-backupalone"...
```

```
Please wait...system reloading is in progress!
```

```
ok
```

```
Reset system!
```

```
Jul 30 2014 17:36:14: %SYS-5-RELOAD: Reload requested
```

**#Configure Device1 to run in the stack mode.**

```
Device1#switch mode virtual
```

```
This command will convert all interface names to naming convention "interface-type member-number/slot/interface" ,
```

```
Please make sure to save current configuration.Do you want to proceed? (yes|no)?y
```

```
Converting interface names Building configuration...
```

```
Copying the startup configuration to backup file named "startup-backupalone"...
```

```
Please wait...system reloading is in progress!
```

```
ok
```

```
Reset system!
```

```
Jul 30 2014 17:36:20: %SYS-5-RELOAD: Reload requested
```

**Step 4: Check the result.**

**#Check on Device0, chain stack system has been formed, and Device0 is the master control device.**

```
Device0#show switch virtual
```

```
Codes: L - local-device,I - isolate-device
```

```
Virtual Switch Mode      : VIRTUAL
```

Virtual Switch DomainId : 10  
Virtual Switch mac-address : 0001.7a6a.001b

----- VST MEMBER INFORMATION -----

CODE	MemberID	Role	Pri	LocalVsl	RemoteVsl
------	----------	------	-----	----------	-----------

L	0	Master	255	vsl-channel 0/1	vsl-channel 1/1
---	---	--------	-----	-----------------	-----------------

	1	Member	200	vsl-channel 1/1	vsl-channel 0/1
--	---	--------	-----	-----------------	-----------------

# 122 MAD

---

## 122.1 Overview

When the virtual switch link interface in the stack system fails, the stack system splits into multiple virtual switch domains, and multiple virtual switch master control devices (hereinafter referred to as master control devices) with the same global configuration appear. This case is called Multi-Active. Since the logical devices from splitting are exactly the same as the original logical device in terms of global configuration, network configuration conflicts will occur, resulting in traffic anomalies. In order to avoid the impact of this case on the business, MAD (Multi-Active Detection) is proposed.

The current stack system supports two MAD modes: MAD LACP and MAD Fast-Hello, which can meet different networking requirements.

The MAD status includes two statuses: Active status and Recovery status. Active status means normal working status, and Recovery status means disabled status. In the disabled status, all L2/3 Ethernet interfaces and VLAN interfaces except the virtual switch link member ports and reserved ports will be shut down by MAD.

When the device receives the MAD packet, it compares the data in the packet with the data of the local logic device. If the VS Domain ID (the virtual switch domain ID of the sender) in the packet is the same as

that of the local logical device, and the Master ID in the packet (the member ID of the master control device in the virtual switch domain where the sender is located) is differed from that of the local logical device, it is considered that multi-active has occurred, and multi-active resolution has begun. According to certain resolution rules, only one logical device in the same virtual switch domain remains in the Active status, and other logical devices enter the Recovery status.

Intermediate device must be used in MAD LACP networking, and intermediate device or direct connection can be used in MAD Fast-Hello networking. If the direct connection mode is used, ensure that there is a direct line between any two virtual switch member devices for multi-active detection, that is, ensure full connection.

## 122.2 MAD Function Configuration

Table 122-1 MAD Function Configuration List

Configuration Task	
Configure MAD LACP function	Configure MAD LACP function
Configure MAD Fast-Hello function	Configure MAD Fast-Hello function
Configure reserved port	Configure reserved port
Configure restoring MAD status to Active status	Configure restoring MAD status to Active status

### 122.2.1 Configure MAD LACP Function

MAD LACP Multi-active detection extends the LACP packet fields to achieve multi-active detection and resolution.

#### Configuration Condition

None

#### Configure MAD LACP Function

Table 122-2 Configuring MAD LACP Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Create dynamic aggregation group	<b>link-aggregation <i>link-aggregation-id</i> mode lacp</b>	Mandatory By default, the aggregation group is not created.
Enter Aggregation Group Configuration Mode	<b>Interface link-aggregation <i>link-aggregation-id</i></b>	-
Enable MAD LACP Function	<b>mad enable</b>	Mandatory By default, the MAD LACP function is not enabled

### Note

- Only the dynamic aggregation group supports enabling the MAD LACP function.
- The intermediate device used in networking must be Our device that supports the LACP packet transparent transmission function.

## 122.2.2 Configure MAD Fast-Hello Function

MAD Fast-Hello multi-active detection protocol packets are customized by our company and directly carry data required by multi-active detection and resolution.

### Configuration Condition

None

### Configure MAD Fast-Hello Function

Table 122-3 Configuring MAD Fast-Hello Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the MAD Fast-Hello packet sending period in normal mode	<b>mad fast-hello normal interval</b> <i>interval-time</i>	Optional By default, the MAD Fast-Hello packet sending period in normal mode is 2000 milliseconds
Configure the MAD Fast-Hello packet sending period in aggressive mode	<b>mad fast-hello aggressive interval</b> <i>interval-time</i>	Optional By default, the MAD Fast-Hello packet sending period in aggressive mode is 500 milliseconds
Configure the duration of aggressive mode	<b>mad fast-hello aggressive duration</b> <i>duration-time</i>	Optional By default, the duration of aggressive mode is 120 seconds
Enter the VLAN configuration mode	<b>vlan</b> <i>vlan-id</i>	-
Configure controlling VLAN	<b>mad fast-hello control-vlan</b>	Mandatory By default, no control VLAN is configured
Enter the global configuration mode.	<b>exit</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	-
Configure the port link type to the Trunk type	<b>switchport mode trunk</b>	Mandatory

Step	Command	Description
		By default, the port link type is the Access type.
Shut down the spanning tree function on the port	<b>no spanning-tree enable</b>	Mandatory By default, the spanning tree function is enabled on the port
Configure control port	<b>mad fast-hello vlan <i>vlan-id</i></b>	Mandatory By default, no control port is configured

### Note

- The control VLAN and control port for MAD Fast-Hello can only be used exclusively for MAD Fast-Hello multi-active detection, and no other services can be configured.
- Shutting down the spanning tree function of the port on the MAD Fast-Hello control port is required.

## 122.2.3 Configure Reserved Port

When MAD is in the Recovery status, the reserved port will not be shut down by MAD. You can configure the ports and interfaces (such as management ports) that need to be in UP status for special purposes as reserved ports.

### Configuration Condition

None

### Configure Reserved Port

Table 122-4 Configuring Reserved Port

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the L2/L3 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  The subsequent configuration takes effect only on the current interface after you enter the L2/L3 Ethernet interface configuration mode, only on the aggregation group after you enter the aggregation group configuration mode, and only on the current port after you enter the interface configuration mode
Enter Aggregation Group Configuration Mode	<b>link-aggregation</b> <i>link-aggregation-id</i>	
Enter the interface configuration mode	<b>interface vlan</b> <i>vlan-id</i>	
Configure reserved port	<b>mad exclude recovery</b>	Mandatory  By default, no reserved port is configured

---

### Note

- The aggregation group that has MAD LACP enabled cannot be configured as reserved port.
- 

## 122.2.4 Configure Restoring MAD Status to Active Status

### Configuration Condition

None

## Configure Restoring MAD Status to Active Status

Table 122-5 Configuring Restoring MAD Status to Active Status

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure restoring MAD status to Active status	<b>mad restore</b>	Mandatory By default, MAD is in Active status

---

### Note

- When the MAD changes to Recovery status, MAD does not process the shut-down ports and interfaces. When the MAD is restored to Active status, only the shut-down ports and interfaces are started up.
- 

## 122.2.5MAD Monitoring and Maintaining

Table 122-6 MAD Monitoring and Maintaining

Command	Description
<b>show mad exclude recovery interface [ switchport   vlan ]</b>	Show the reserved port configured
<b>show mad fast-hello</b>	Show MAD Fast-Hello information
<b>show mad lacp</b>	Show MAD LACP information
<b>show mad status</b>	Show MAD status

## 122.3 Typical Configuration Example of MAD

### 122.3.1 Configure MAD LACP Function

#### Network Requirements

- Device0 and Device1 form a stack system with Device0 as the master control device, and PC 1 accesses the IP Network through the stack system;
- After the MAD LACP function is configured, PC 1 can access the IP Network properly after Device1 is separated from the stack system due to a fault of the virtual switch link interface. Service exceptions due to network configuration conflicts are not caused.

#### Network Topology

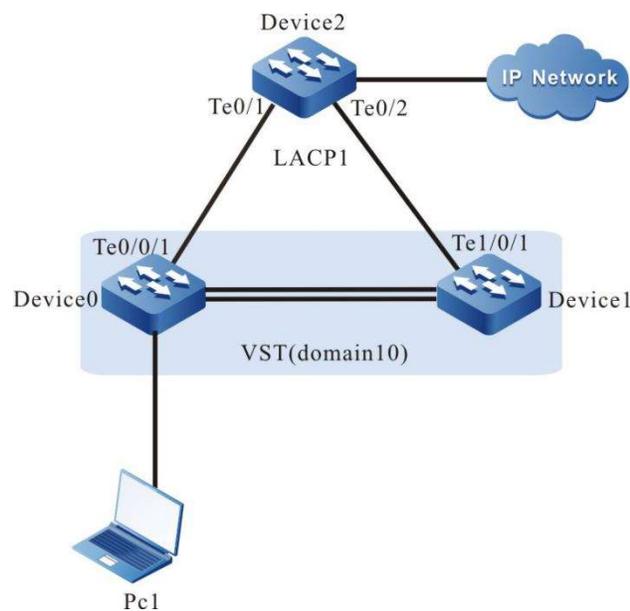


Figure 122-1 Network Topology for Configuring MAD LACP

#### Configuration Steps

Step 1: Device0 and Device1 form a stack system with Device0 as the master control device.

Omitted

Step 2: Configure the MAD LACP function on Device0.

#On Device0, create VLAN 2 and dynamic aggregation group 1, configure the link type of the aggregation group 1 to Trunk to allow services of VLAN 2 to pass.

```
Device0#configure terminal
Device0(config)#vlan 2
Device0(config-vlan2)#exit
Device0(config)#link-aggregation 1 mode lacp
Device0(config)#interface link-aggregation 1
Device0(config-link-aggregation1)#switchport mode trunk
Device0(config-link-aggregation1)#switchport trunk allowed vlan add 2
Device0(config-link-aggregation1)#exit
```

**#On Device0, add ports tengigabitethernet0/0/1 and gigabitethernet1/0/1 into the aggregation group 1.**

```
Device0(config)#interface tengigabitethernet 0/0/1,1/0/1
Device0(config-if-range)#link-aggregation 1 active
Device0(config-if-range)#exit
```

**#Enable the MAD LACP function on the aggregation group 1 of Device0.**

```
Device0(config)#interface link-aggregation 1
Device0(config-link-aggregation1)#mad enable
Device0(config-link-aggregation1)#exit
```

**Step 3: Configure Device2.**

**#On Device2, create VLAN 2 and dynamic aggregation group 1, configure the link type of the aggregation group 1 to Trunk to allow services of VLAN 2 to pass.**

```
Device2#configure terminal
Device2(config)#vlan 2
Device2(config-vlan2)#exit
Device2(config)#link-aggregation 1 mode lacp
Device2(config)#interface link-aggregation 1
Device2(config-link-aggregation1)#switchport mode trunk
Device2(config-link-aggregation1)#switchport trunk allowed vlan add 2
Device2(config-link-aggregation1)#exit
```

**#On Device2, add ports tengigabitethernet0/1 and gigabitethernet0/2 into the aggregation group 1.**

```
Device2(config)#interface tengigabitethernet 0/1,0/2
Device2(config-if-range)#link-aggregation 1 active
Device2(config-if-range)#exit
```

**Step 4: Check the result.**

**#View the MAD LACP information on Device0.**

```
Device0#show mad lacp
-----MAD-LACP INFORMATION-----
Link-aggregation   Mad state
-----
1                   enable
```

#After Device1 is separated from the stack system due to the fault of the virtual switch link interface, the MAD status of the stack system using Device0 as the master control device changes to Active status, and the MAD status of the stack system using Device1 as the master control device changes to Recovery status.

```
Device0#show mad status
MAD status: active
```

```
Device1#show mad status
MAD status: recovery
```

#PC 1 can access the IP Network.

### 122.3.2 Configure MAD Fast-Hello Function

#### Network Requirements

- Device0 and Device1 form a stack system with Device0 as the master control device;
- After the MAD Fast-Hello function is configured, and after Device1 is separated from the stack system due to the fault of the virtual switch link interface, service exceptions due to network configuration conflicts will not be caused.

#### Network Topology

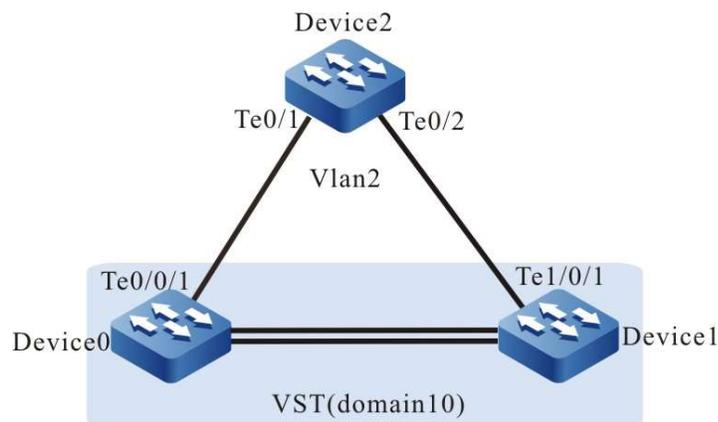


Figure 122-2 Network Topology for Configuring MAD Fast-Hello

#### Configuration Steps

Step 1: Device0 and Device1 form a stack system with Device0 as the master control device.

Omitted

Step 2: Configure the MAD Fast-Hello function on Device0.

#Create VLAN 2 on Device0 and configure it as MAD Fast-Hello control VLAN.

```
Device0#configure terminal
```

```
Device0(config)#vlan 2
```

```
Device0(config-vlan2)#mad fast-hello control-vlan
```

```
Device0(config-vlan2)#exit
```

#Configure on Device0, the like types of ports tengigabitethernet0/0/1 and tengigabitethernet1/0/1 as Trunk, and join the MAD Fast-Hello control VLAN.

```
Device0(config)#interface tengigabitethernet 0/0/1,1/0/1
```

```
Device0(config-if-range)#switchport mode trunk
```

```
Device0(config-if-range)#mad fast-hello vlan 2
```

```
Device0(config-if-range)#exit
```

#On Device0, shut down the spanning tree function of the ports tengigabitethernet0/0/1 and gigabitethernet1/0/1.

```
Device0(config)#interface tengigabitethernet 0/0/1,1/0/1
```

```
Device0(config-if-range)#no spanning-tree enable
```

```
Device0(config-if-range)#exit
```

Step 3: Configure Device2.

#On Device2, create VLAN 2, configure the link types of ports tengigabitethernet0/1 and gigabitethernet0/2 as Trunk to allow services of VLAN 2 to pass.

```
Device2#configure terminal
```

```
Device2(config)#vlan 2
```

```
Device2(config-vlan2)#exit
```

```
Device2(config)#interface tengigabitethernet 0/1,0/2
```

```
Device2(config-if-range)#switchport mode trunk
```

```
Device2(config-if-range)#switchport trunk allowed vlan add 2
```

```
Device2(config-if-range)#exit
```

#On Device2, shut down the spanning tree function of the ports tengigabitethernet0/1 and gigabitethernet0/2.

```
Device2(config)#interface tengigabitethernet 0/1,0/2
```

```
Device2(config-if-range)#no spanning-tree enable
```

```
Device2(config-if-range)#exit
```

Step 4: Check the result.

**#View MAD Fast-Hello enabling on Device0.**

```
Device0#show mad fast-hello
```

```
MAD Fast-Hello Information:
```

```
Normal interval : 2000 ms(default: 2000)
```

```
Aggressive interval : 500 ms(default: 500)
```

```
Aggressive duration : 120 s (default: 120)
```

```
Control vlan : 2
```

```
-----  
Interface Control vlan
```

```
-----  
te0/0/1 2
```

```
te1/0/1 2
```

**#After Device1 is separated from the stack system due to the fault of the virtual switch link interface, the MAD status of the stack system using Device0 as the master control device changes to Active status, and the MAD status of the stack system using Device1 as the master control device changes to Recovery status.**

```
Device0#show mad status
```

```
MAD status: active
```

```
Device1# show mad status
```

```
MAD status: recovery
```

# 123 MVST

---

## 123.1 Overview

At present, VST (Virtual Switching Technologies, which will combine crosswise multiple physical devices into one virtual device) technology because of its high reliability, ease of management and other characteristics gradually become a necessary networking technology to LAN. VST technology realizes the centralized management of multiple devices at the same level, but there is still the problem of decentralized management of devices on the multi-level network. Especially in the typical two-level local area network, the access layer uses numerous access devices that are enormous in amount and highly dispersed and need sequential maintenance and management, making the management work be cumbersome. Additionally, assigning each of these devices an IP address will consume a lot of IP address resources, which is undoubtedly a waste with IP address resources running short at present.

To solve the above problems, MVST (Mix Virtual Switching Technology, vertical management virtualization technology) technology is proposed. As shown in the figure below, VST technology is used for the core layer of LAN to virtualize multiple devices into one logical device, while Mix Virtual Switching Technology (MVST), a vertical management virtualization technology, is used for the vertical layer. MVST virtualizes all devices of the entire LAN into one logical device, constituting a centralized management domain (MVST domain). The management domain provides one external management IP address and the ability to manage and access each device on the LAN. In this way, "one network and one device" is truly achieved, one network has one IP, and the entire LAN can be readily managed with one device, thereby simplifying management.

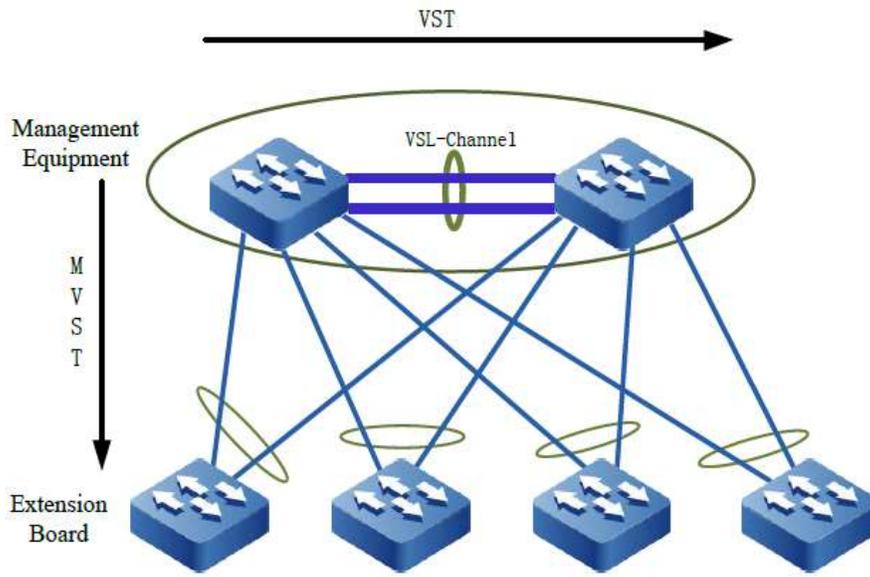


Figure 123-1 MVST Physical Network View

MVST defines three device roles depending on the different statuses and functions of devices in the LAN.

- Management device (MVST master) : responsible for configuring, managing, and monitoring all devices on the LAN.
- Extension board (MVST Slave slot): extension board for LAN that can be centrally configured and managed by the management device.
- Candidate board (MVST Candidate): not added to the MVST domain, but qualified to be extension board.

The management device in the MVST domain uses the MVST detection protocol to discover extension boards and uses the MVST topology collection protocol to collect information about each extension card in the MVST domain and draw a LAN topology. The management device adds the joined devices to the MVST domain based on the topology.

After the extension board is added to the MVST domain, users can log in to the control interface of the management device using the IP address of the management device to centrally manage the entire LAN. In addition to general configuration management, MVST technology provides the following features:

#### 1) Template-based Configuration

In application scenarios, some common basic configurations need to be applied to all extension boards in the MVST domain. You can edit these configurations to a configuration template, and then the management device issues the configuration template to the extension boards, so the extension boards are completed with the common basic configurations.

## 2) autoconfiguration

The management device backs up the startup configuration file of the extension board to the local storage medium. When the extension board is faulty and needs to be replaced with a new one, the new extension board is directly connected to the LAN through the same port without any configuration. The management device automatically sends the backup configuration file to the extension board. After the extension board is configured, the network is quickly restored.

## 3) One-click Configuration

The management device can start up Dot1x, storm control, DHCP Snooping, and Arp-check functions of all extension boards in the MVST domain by one click.

## 4) Auto upgrade

The management device prepares the IOS of the extension board in advance. When the extension board joins the MVST domain, the management device automatically detects the consistency between the current running version of the extension board and the auto upgrade version. The background performs auto upgrade in case of inconsistency. Log information is printed if the user visual interface is shown. During the upgrade process of the extension board, the user can still manage the management device or extension board to achieve both upgrade and configuration.

## 5) Password Dynamic Management

The login passwords of all extension boards in the MVST domain are dynamically generated by the management device. After the extension board successfully joins the MVST domain, the management device generates a dynamic password and sends the password to the extension board. During the operation of the extension board, if you need to log in directly through the console, the login password can only be obtained through the management device, which strengthens the security of the local area network.

## 123.2 MVST Function Configuration

Table 123-1 MVST Function Configuration List

Configuration Task	
Configure MVST basic functions	Configure the management device
	Configure extension boards
Configure MVST parameters	Configure sending interval for inspection packets
	Configure neighbor aging time

Configuration Task	
	Configure the keepalive interval of extension boards
	Configure connection status timeout for extension boards
	Configure topology parameters
Configure MVST features	Configure the upgrade function
	Configure the template function
	Configure the auto binding configuration function
	Configure personalized configuration
	Configure the device group function
	Configure the log function

### 123.2.1 Configure MVST Basic Functions

When the users need to manage devices in a certain domain through MVST technology, they can configure MVST. In the various configuration tasks of MVST, the MVST function must be enabled before other function configurations can take effect.

#### Configuration Condition

None

#### Configure the Management Device

The management device is the nerve center of MVST. It provides one management tunnel for the MVST domain, through which the administrator realizes the centralized management of the devices in the specified domain.

Table 123-2 Configuring the Management Device

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable the MVST function	<b>mvst enable</b>	Mandatory By default, the MVST function is disabled
Configure the specified device as the management device for the MVST domain	<b>mvst master</b>	Mandatory By default, no management device is specified
Configure MVST domain name	<b>mvst domain-name</b> <i>domain-name</i>	Optional By default, the MVST domain name is "mvst-1"
Create MVST dedicated aggregation port	<b>mvst link-aggregation</b>	Create MVST link aggregation port
Add aggregation group members	<b>mvst interface</b> <i>interface-name join link-aggregation link-aggregation-id active</i>	Add member ports to the MVST aggregation port
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected. After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes
Enter Aggregation Group Configuration Mode	<b>Interface link-aggregation</b> <i>link-aggregation-id</i>	

Step	Command	Description
		effect only within the aggregation group.
Configure the downlink port to enable MVST inspection	<b>mvst inspection</b>	Mandatory By default, the port's MVST inspection function is disabled

### Configure Extension Boards

When the users want to manage a certain device through MVST, they can configure the device as an extension board of the MVST domain. The case-type device enables the MVST function, and starts up the MVST inspection function under port or link aggregation.

Table 123-3 Configuring Extension Boards

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable the MVST function	<b>mvst enable</b>	Mandatory By default, the MVST function is disabled
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected. After you enter the
Enter Aggregation Group Configuration Mode	<b>Interface link-aggregation</b> <i>link-aggregation-id</i>	layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes

Step	Command	Description
		effect only within the aggregation group.
Configure the downlink port to enable MVST inspection	<b>mvst inspection</b>	Mandatory  By default, the port's MVST inspection function is disabled

## 123.2.2 Configure MVST Parameters

### Configuration Condition

Before configuring MVST parameters, do the following for the first time:

- Configure the management device.

### Configure Sending Interval for Inspection Packets

The device that enables the MVST function periodically sends inspection packets to discover the devices connected to it, and extracts key information from the inspection packets to form its own neighbor device information table.

Table 123-4 Configuring Sending Interval for Inspection Packets

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure sending interval for MVST inspection packets	<b>mvst inspection timer</b> <i>timer-value</i>	Mandatory  By default, the interval for sending MVST inspection packets is 10 seconds

### Configure Neighbor Aging Time

The neighbor aging time refers to the survival time of the local device information on the neighbor device, enabling the neighbor device to delete the local device information after the local device survival time expires.

Table 123-5 Configuring Neighbor Aging Time

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the aging time of local device information in neighbor devices	<b>Mvst inspection aging-time</b> <i>aging-time-value</i>	Mandatory  By default, the aging time of local device information in neighbor devices is 30 seconds

### Configure the Keepalive Interval of Extension Boards

After the extension board joins the MVST domain, the management device and the extension board start to exchange keepalive packets. By default, keepalive packets are exchanged every 8 seconds. If the management device cannot receive 3 keepalive packets of the extension board continuously, the extension board will be transitioned from the Active (online) status to the Connect (connect) status.

Table 123-6 Configuring the Keepalive Interval of Extension Boards

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the keepalive interval of extension boards	<b>mvst handtime</b> <i>handtime-value</i>	Mandatory  By default, the keepalive interval of extension boards is 8 seconds

### Configure Connection Status Timeout for Extension Boards

If the management device receives a keepalive packet sent by the extension board within the valid time of the connection state, it will transition the extension board from the Connect status to the Active status; if it has not received the keepalive packet sent by the extension board, it transitions the extension board from the Connect status to the Disconnect status.

The management device no longer sends the keepalive packet to the extension board in the Disconnect status until it receives the keepalive packet sent by the extension board again.

Table 123-7 Configuring Connection Status Timeout for Extension Boards

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure Connect status timeout for extension boards	<b>mvst holdtime</b> <i>holdtime-value</i>	Mandatory  By default, the Connect status timeout of the extension board is 80 seconds

### Configure Topology Parameters

After the MVST domain is established, the management device regularly collects the topology information of the entire MVST domain through the topology request packet. When the topology request packet spreads across the network, numerous network devices will receive the topology request packet at the same time and send topology response packets at the same time, which may cause network congestion. In order to alleviate this problem, after the management device waits for the delay time for the device to forward the topology collection request packet on each port, the second port starts to forward the topology request packet, and so on, until the last port finishes forwarding.

Table 123-8 Configuring Topology Parameters

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the topology collection period	<b>mvst topo hello-time</b> <i>hello-time-value</i>	Mandatory  By default, the topology collection period is 30 seconds.

Step	Command	Description
Configure the management device port to delay the topology collection time	<b>mvst topo port-delay-time</b> <i>port-delay-time-value</i>	Optional  By default, delay time for the management device port to collect topology is 100ms

### 123.2.3 Configure MVST Features

#### Configuration Condition

Before configuring MVST features, do the following:

- Configure MVST basic functions

#### Configure the Upgrade Function

The upgrade function refers to the management device upgrading the system image ios file or Bootloader file of the extension board.

There are two manners to upgrade the system image file or Bootloader file of the extension board:

1. Auto upgrade. When the extension board successfully joins the MVST domain, the management device automatically checks the consistency between the current running version of the extension board and the version in the auto upgrade configuration. The extension board is automatically upgraded in case of inconsistency. This upgrade manner currently only supports upgrading the IOS file for the extension board.
2. Manual upgrade. Users can upgrade the system image file or Monitor file of the extension board in real time by way of the command line according to the real-time requirements.

Table 123-9 Configuring the Upgrade Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure auto upgrade	<b>mvst auto update image { path/image-name   image-name } [ ip-address { ftp user-</b>	Mandatory

Step	Command	Description
	name user-password   tftp } [reload [write ]]reload [write ]]	By default, there is no auto upgrade configuration.
Enter the privileged user mode.	exit	-
Configure manual upgrade for extension boards	mvst update slave-slot slave-slot-id { image   bootloader } { path/filename   filename } [ ip-address { ftp user-name user- password   tftp } [ reload ]   reload ] or  mvst update device- group device-group-id { image   bootloader } { path/filename   filename } [ ip-address { ftp user-name user- password   tftp } [ reload ]   reload ]	Optional

---

### Note

- Before configuring auto upgrade, you need to make sure that the version file exists.
- 

### Configure the Template Function

The template function facilitates batch configuration management, which brings convenience to network maintenance. Users can edit the common basic configuration into one txt text file according to the network operation and maintenance requirements, the management device then issues this text file to the extension board, and the extension board completes the common basic configuration.

Table 123-10 Configuring the Template Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Specify a configuration template	<b>mvst configure template</b> <i>template-name</i>	Mandatory By default, no configuration template is specified.
Configure the management device to issue the configuration template to the extension board	<b>mvst apply configure template {service-group service-group-id   slave-slot { slave-slot-id   all } }</b>	Optional

---

### Note

- After the management device has issued the configuration template to the extension board, it should execute the command **write slave-slot** or **write device-group** to enable all extension boards to save the current configuration information to the startup configuration file.
- 

### Configure the Auto Binding Configuration Function

The management device backs up the startup configuration files of all extension boards in the MVST domain to the local storage medium through the auto binding configuration function. When the extension board needs to be replaced due to failure or other reasons, the new extension board can be automatically configured through the startup configuration file backed up.

Table 123-11 Configuring the Auto Binding Configuration Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Configure the port to bind to the startup configuration file	<b>mvst bind startup interface</b> <i>{interface-list   link-aggregation link-aggregation-id}</i>   <b>all</b>	Mandatory  By default, the port is not bound to the startup configuration file.

### Configure Personalized Configuration

The extension board in the MVST domain will undertake different network services due to the network environment in which they are located, so the configuration of the extension board needs to be personalized. The administrator can log in to the virtual configuration interface of the extension board through the management device to complete the configuration management for the extension board.

Table 123-12 Configuring Personalized Configuration

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configuration to manage extension boards	<b>configure slave-slot</b> <i>slave-slot-id</i>	Mandatory  Log in to the virtual configuration interface of the extension board
Enter the privileged user mode.	<b>exit</b>	-
Configure the extension board to save the current configuration information to the startup configuration file	<b>write slave-slot</b> <i>slave-slot-id</i>	Optional

### Configure the Device Group Function

When all extension boards in a device group need to achieve the same function, batch configuration management can be completed by configuring the device group. The administrator can log in to the virtual configuration interface of the device group configuration prototype through the management device to complete the configuration management for the device group.

Table 123-13 Configuring the Device Group Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the device group	<b>configure device-group</b> <i>device-group-id slave-slot slave-slot-id</i>	Mandatory The administrator logs in to the virtual configuration interface of the device group configuration prototype
Enter the privileged user mode.	<b>exit</b>	-
Configure all extension boards in the device group to save the current configuration information to the startup configuration file	<b>write device-group</b> { <i>device-group-id</i>   <b>all</b> }	Optional

### Configure the Service Group Function

When all extension boards in a service group need to achieve the same function, batch configuration management can be completed by configuring the service group, such as configuring the same configuration template. The administrator can log in to the service group interface through the management device to manage the configuration of the service group.

Table 123-14 Configuring the Service Group Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the service group	<b>Mvst service-group</b> <i>service-group-id</i>	Mandatory Create and enter the service group
Add Members	<b>In service configuration mode</b> <b>slave-slot</b> <i>slave-slot-id</i>	Mandatory Add the extension board to the service group
Specify a service group configuration template	<b>configure template</b> <i>/flash/filepath</i>	Optional Specify all next extension boards in the service group to execute the same configuration template
Enter the privileged user mode.	<b>exit</b>	-

### Configure the Log Function

The MVST log function means that the extension board sends the log information of the local device to the management device. The administrator can modify the range of log levels sent by the extension board to the management device in real time according to the requirements of the network environment.

Table 123-15 Configuring the Log Function

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Configure the log level sent by the extension board to the management device	<b>mvst slave-slot logging</b> [ <i>logging-level1</i> <i>logging-level2</i> ]	Mandatory  By default, the log level sent by the extension board to the management device is 0-5

## 123.2.4 MVST Monitoring and Maintaining

Table 123-16 MVST Monitoring and Maintaining

Command	Description
<b>show mvst auto-update config</b>	Show auto upgrade configuration information
<b>show mvst device-group</b> [ <i>device-group-id</i> ]	Show the configuration execution information of the specified device group
<b>show mvst service-group</b> [ <i>service -group-id</i> ]	Show the information of service group or specified business group
<b>show mvst inspection</b>	Show neighbor information of this device
<b>show mvst inspection opened</b>	Show the port with the MVST inspection function started up
<b>show mvst inspection queue</b>	Show MVST inspection packet-receiving queue information
<b>show mvst slave-slot</b>	Show the information of extension boards in the MVST domain

Command	Description
<b>show mvst slave-slot</b> <i>slave-slot-id</i> <b>command</b>	Show some key running information of the specified extension board
<b>show mvst slave-slot logging</b>	Show the range of log levels sent by the extension boards to the management device
<b>show mvst slave-slot password</b>	Show the login password table for the extension boards
<b>show mvst slave-slot</b> { <i>slave-slot-id</i> <b>use-info</b>   <b>use-info</b> }	Show the use information of the extension board numbers
<b>show mvst startup bind info</b>	Show port binding information
<b>show mvst statistics</b>	Show MVST packet receiving and sending statistics
<b>show mvst summary</b>	Show summary information of MVST domain
<b>show mvst topo config</b>	Show topology parameter configuration information
<b>show mvst topo information</b> [ <b>slave-slot</b> <i>slave-slot-id</i> ]	Show topology information
<b>show mvst tunnel</b>	Show the information of the tunnel between the management device and the extension boards in the MVST domain
<b>show mvst upgrade-information</b> { <b>device-group</b> <i>device-group-id</i>   <b>slave-slot</b> { <b>all</b>   <i>slave-slot-id</i> } }	Show the upgrade status information of the extension board
<b>show mvst write-information</b> <b>device-group</b> { { <i>device-group-id</i>   <b>all</b> }   <b>slave-slot</b> <i>slave-slot-id</i> }	Show the status information of the extension board about saving the current configuration

Command	Description
<b>show running-config slave-slot</b> <i>slave-slot-id</i>	Show configuration information of the current configuration of the extension board
<b>show startup-config slave-slot</b> <i>slave-slot-id</i>	Show the content of the startup configuration file of the extension board

## 123.3 Typical Configuration Example of MVST

### 123.3.1 Configure Auto Upgrade Inspection

#### Network Requirements

- Device1 and Device2 form a stack system as MVST management device, Device3, Device4, and Device5 are used as extension boards, and the last two ports of the extension boards are connected to the MVST management device;
- The management device configures auto upgrade inspection. When Device3, Device4, and Device5 are added as extension boards to the MVST domain, the extension boards can be automatically upgraded.

#### Network Topology

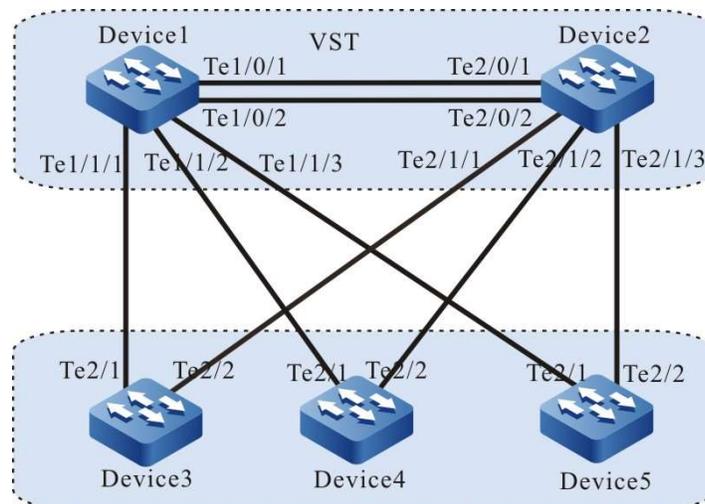


Figure 123-2 Configuring Auto Upgrade Inspection

#### Configuration Steps

Step 1: Configure the VST system.

**#On Device1, configure the virtual switch member device ID as 1, and configure the domain ID as 10 and the priority as 255.**

```
Device1#configure terminal
Device1(config)#switch virtual member 1
Do you want to modify member id(Yes|No)?y
% Member ID 1 config will take effect only after the exec command 'switch mode virtual' is issued
Device1(config-vst-member-1)#domain 10
% Domain ID 10 config will take effect only after the exec command 'switch mode virtual' is issued
Device1(config-vst-member-1)#priority 255
Device1(config-vst-member-1)#exit
```

**#On Device1, create virtual switch link interface 1, and add ports tengigabitethernet0/1 and tengigabitethernet0/2 to the virtual switch link interface 1.**

```
Device1(config)#vsl-channel 1
Device1(config-vsl-channel-1)#exit
Device1(config)#interface tengigabitethernet 0/1
Device1(config-if-tengigabitethernet0/1)#vsl-channel 1 mode on
Device1(config-if-tengigabitethernet0/1)#exit
Device1(config)#interface tengigabitethernet 0/2
Device1(config-if-tengigabitethernet0/2)#vsl-channel 1 mode on
Device1(config-if-tengigabitethernet0/2)#exit
```

**#Save the configuration on Device1.**

```
Device1#write
Are you sure to overwrite /flash/startup (Yes|No)?y
Building Configuration...done
Write to startup file ... OK
Write to mode file... OK
```

**#On Device2, configure the virtual switch member device ID as 1, and configure the domain ID as 10 and the priority as 200.**

```
Device2#configure terminal
Device2(config)#switch virtual member 2
Do you want to modify member id(Yes|No)?y
% Member ID 2 config will take effect only after the exec command 'switch mode virtual' is issued
Device2(config-vst-member-2)#domain 10
% Domain ID 10 config will take effect only after the exec command 'switch mode virtual' is issued
Device2(config-vst-member-2)#priority 200
Device2(config-vst-member-2)#exit
```

**#On Device2, create virtual switch link interface 1, and add ports tengigabitethernet1/1 to the virtual switch link interface 1.**

```
Device2(config)#vsl-channel 1
Device2(config-vsl-channel-1)#exit
Device2(config)#interface tengigabitethernet 0/1
Device2(config-if-tengigabitethernet0/1)#vsl-channel 1 mode on
Device2(config-if-tengigabitethernet0/1)#exit
Device2(config)#interface tengigabitethernet 0/2
Device2(config-if-tengigabitethernet0/2)#vsl-channel 1 mode on
Device2(config-if-tengigabitethernet0/2)#exit
```

**#Save the configuration on Device2.**

```
Device2#write
Are you sure to overwrite /flash/startup (Yes|No)?y
Building Configuration...done
Write to startup file ... OK
Write to mode file... OK
```

**#Configure Device1 to run in the stack mode.**

```
Device1#switch mode virtual
This command will convert all interface names to naming convention "interface-type member-number/slot/interface" ,
Please make sure to save current configuration.Do you want to proceed? (yes|no)?y
Converting interface names Building configuration...
Copying the startup configuration to backup file named "startup-backupalone"...
Please wait...system reloading is in progress!
ok
Reset system!
%SYS-5-RELOAD: Reload requested
```

**#Configure Device2 to run in the stack mode.**

```
Device2#switch mode virtual
This command will convert all interface names to naming convention "interface-type member-number/slot/interface" ,
Please make sure to save current configuration.Do you want to proceed? (yes|no)?y
Converting interface names Building configuration...
Copying the startup configuration to backup file named "startup-backupalone"...
Please wait...system reloading is in progress!
ok
Reset system!
%SYS-5-RELOAD: Reload requested
```

**#After reboot. Check on Device1, chain stack system has been formed, and Device1 is the master control device of the stack system.**

```
Device1#show switch virtual
Codes: L - local-device,I - isolate-device

Virtual Switch Mode      : VIRTUAL
Virtual Switch DomainId  : 10
Virtual Switch mac-address : 0001.7a6a.0255
```

```
----- VST MEMBER INFORMATION -----
CODE MemberID Role  Pri LocalVsl  RemoteVsl
-----
L  1    Master 255 vsl-channel 1/1  vsl-channel 2/1
   2    Member 200 vsl-channel 2/1  vsl-channel 1/1
```

**Step 2: Configure the basic functions of MVST.**

**#Configure the stack system as MVST management device on Device1.**

```
Device1(config)#mvst enable
%MVST-NOTIFY-5: MVST is enabled !
Device1(config)#mvst master
Device1(config)#mvst domain-name test
```

**#Configure stack system link aggregation on Device1 and start up MVST inspection.**

```
Device1(config)#mvst link-aggregation 1 mode lacp
Device1(config)# mvst interface tengigabitethernet 1/1/1,2/1/1 join link-aggregation 1 active
Device1(config)#interface link-aggregation 1
Device1(config-link-aggregation1)#mvst inspection
Device1(config-link-aggregation1)#exit
Device1(config)#mvst link-aggregation 2 mode lacp
Device1(config)# mvst interface tengigabitethernet 1/1/2,2/1/2 join link-aggregation 2 active
Device1(config)#interface link-aggregation 2
Device1(config-link-aggregation2)#mvst inspection
Device1(config-link-aggregation2)#exit
Device1(config)#mvst link-aggregation 3 mode lacp
Device1(config)# mvst interface tengigabitethernet 1/1/3,2/1/3 join link-aggregation 3 active
Device1(config)#interface link-aggregation 3
Device1(config-link-aggregation3)#mvst inspection
Device1(config-link-aggregation3)#exit
```

**#Enable MVST function on Device3.**

```
Device3#configure terminal
```

```
Device3#configure terminal
Device3(config)#mvst enable
%MVST-NOTIFY-5: MVST is enabled !
Device3Device3(config)#mvst link-aggregation 1 mode lacp
Device3(config)# mvst interface tengigabitethernet 2/1,2/2 join link-aggregation 1 active
Device3(config)#interface link-aggregation 1
Device3(config-link-aggregation1)#mvst inspection
Device3(config-link-aggregation1)#exit

%MVST-NOTIFY-5: interface tengigabitethernet2/1 and interface tengigabitethernet2/2 join link-aggregation 1 successfully.
```

#### **#Enable MVST function on Device4.**

```
Device4#configure terminal
Device4(config)#mvst enable
%MVST-NOTIFY-5: MVST is enabled !
Device4(config)#mvst link-aggregation 2 mode lacp
Device4(config)# mvst interface tengigabitethernet 2/1,2/2 join link-aggregation 2 active
Device4(config)#interface link-aggregation 2
Device4(config-link-aggregation2)#mvst inspection
Device4(config-link-aggregation2)#exit

%MVST-NOTIFY-5: interface tengigabitethernet2/1 and interface tengigabitethernet2/2 join link-aggregation 2 successfully.
```

#### **#Enable MVST function on Device5.**

```
Device5#configure terminal
Device5(config)#mvst enable
%MVST-NOTIFY-5: MVST is enabled !
Device5(config)#mvst link-aggregation 3 mode lacp
Device5(config)# mvst interface tengigabitethernet 2/1,2/2 join link-aggregation 3 active
Device5(config)#interface link-aggregation 3
Device5(config-link-aggregation3)#mvst inspection
Device5(config-link-aggregation3)#exit

%MVST-NOTIFY-5: interface tengigabitethernet2/1 and interface tengigabitethernet2/2 join link-aggregation 3 successfully.
```

Step 3: Configure auto upgrade inspection.

**#Configure auto upgrade inspection on Device1, specify the version of the extension board to be upgraded, and add clear, reload, and write parameters.**

```
Device1(config)# mvst auto update image /flash/sp26-g-9.66.0.11(R).pck reload write
```

**#Check the configuration result on Device1.**

## Device1(config)# show mvst auto-update config

OPTION Codes:

- R -- Reload slave slot when update slave slot successfully
- W -- Save slave slot current configuration to startup-config

ID	OPTION	IMAGE-NAME	IMAGE-PATH
1	None	sp25-g-9.6.1.1(R).pck	/flash/sp25-g-9.6.1.1(R).pck
2	R	sp23-g-9.6.1.1(R).pck	/flash/sp23-g-9.6.1.1(R).pck
3	RW	sp26-g-9.6.0.1(R).pck	/flash/sp26-g-9.6.0.1(R).pck

Step 4: connect the extension boards Device3, Device4, and Device5 to the MVST domain, and allow auto upgrade if the inspected current version of Device3 is inconsistent with the version to be upgraded. Skip auto upgrade if the inspected versions of Device4 and Device5 are inconsistent.

#Connect Device3, Device4, and Device5 to the MVST domain in turn, and after the devices are connected, check the MVST result on Device1.

#Check the MVST result on Device1, you can see that Device3, Device4, and Device5 are added to the MVST domain in the form of extension boards. The slots are Slave-slot0, Slave-slot1, and Slave-slot2, and their host names change to switch-ss0, switch-ss1, switch-ss2.

Device1#show mvst topo information

role	domain-name	interface	mac	device-type	host-name
Slave-slot	test	link-aggregation 1	0001.7a63.bd76	NSS4330-56TXF(V1)	switch-ss0
Slave-slot	test	link-aggregation 2	0001.7a64.72aa	NSS4330-56TXF(V1)	switch-ss1
Slave-slot	test	link-aggregation 3	0001.7a63.bd43	NSS4330-56TXF(V1)	switch-ss2
Master	test		0001.7a6a.0258	NSS5810-50TXFP(V1)	Device1

#On Device1, you can check the upgrade status of the extension board in real time. Device3 is in the upgrade status. After Device3 is successfully upgraded, restart it. Device4 and Device5 are not upgraded.

Device1#show mvst upgrade-information slave-slot all

Slave slot upgrade information:

ss-id	upgrade-type	upgrade-status	start-time	over-time	hostname
-------	--------------	----------------	------------	-----------	----------

```

0 image downloading JAN/27/2015 14:58:24 switch-ss0
1 none none switch-ss1
2 none none switch-ss2

```

#Device3 is upgraded successfully. Save the configuration and reboot.

```

Device1#
%MVST-UPDATE_NOTIFY-5: Update slave slot 0 image successfully.
%MVST-WRITE_RESULT-5: The slave slot 0 write to startup file successfully.
%MVST-NOTIFY_RELOAD-3: Slave slot 0 mpu is going to reload.

```

### 123.3.2 Configure Auto Issue of Common Template

#### Network Requirements

- Device1 and Device2 form a stack system as MVST management device, Device3, Device4, and Device5 are used as extension boards, and the last two ports of the extension boards are connected to the MVST management device;
- Configure Device3 as a template switch and use its configuration as a common template configuration. When Device4 and Device5 are connected to the MVST domain, the configuration template will be automatically issued;
- Change the configuration of Device3, recollect it as a common configuration template, and force it to be issued to Device4 and Device5.

#### Network Topology

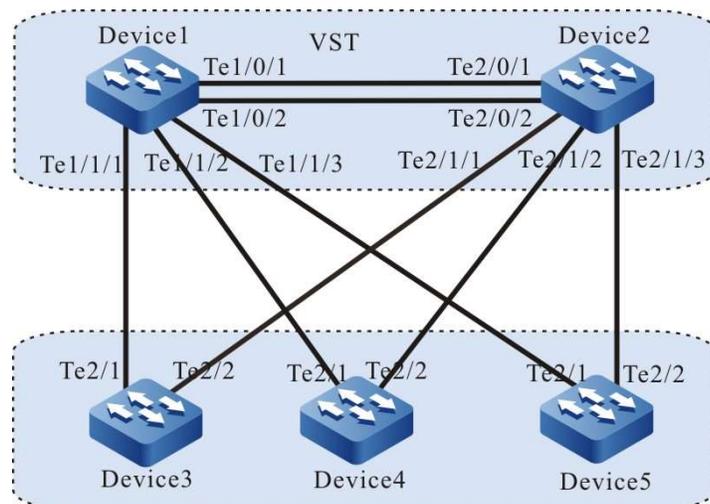


Figure 123-3 Configuring Auto Issue of Common Template

#### Configuration Steps

Step 1: Configure the VST system.

**#On Device1, configure the virtual switch member device ID as 1, and configure the domain ID as 10 and the priority as 255.**

```
Device1#configure terminal
Device1(config)#switch virtual member 1
Do you want to modify member id(Yes|No)?y
% Member ID 1 config will take effect only after the exec command 'switch mode virtual' is issued
Device1(config-vst-member-1)#domain 10
% Domain ID 10 config will take effect only after the exec command 'switch mode virtual' is issued
Device1(config-vst-member-1)#priority 255
Device1(config-vst-member-1)#exit
```

**#On Device1, create virtual switch link interface 1, and add ports tengigabitethernet0/1 and tengigabitethernet0/2 to the virtual switch link interface 1.**

```
Device1(config)#vsl-channel 1
Device1(config-vsl-channel-1)#exit
Device1(config)#interface tengigabitethernet 0/1
Device1(config-if-tengigabitethernet0/1)#vsl-channel 1 mode on
Device1(config-if-tengigabitethernet0/1)#exit
Device1(config)#interface tengigabitethernet 0/2
Device1(config-if-tengigabitethernet0/2)#vsl-channel 1 mode on
Device1(config-if-tengigabitethernet0/2)#exit
```

**#Save the configuration on Device1.**

```
Device1#write
Are you sure to overwrite /flash/startup (Yes|No)?y
Building Configuration...done
Write to startup file ... OK
Write to mode file... OK
```

**#On Device2, configure the virtual switch member device ID as 1, and configure the domain ID as 10 and the priority as 200.**

```
Device2#configure terminal
Device2(config)#switch virtual member 2
Do you want to modify member id(Yes|No)?y
% Member ID 2 config will take effect only after the exec command 'switch mode virtual' is issued
Device2(config-vst-member-2)#domain 10
% Domain ID 10 config will take effect only after the exec command 'switch mode virtual' is issued
Device2(config-vst-member-2)#priority 200
Device2(config-vst-member-2)#exit
```

**#On Device2, create virtual switch link interface 1, and add ports tengigabitethernet1/1 to the virtual switch link interface 1.**

```
Device2(config)#vsl-channel 1
Device2(config-vsl-channel-1)#exit
Device2(config)#interface tentengigabitethernet 0/1
Device2(config-if-tentengigabitethernet0/1)#vsl-channel 1 mode on
Device2(config-if-tentengigabitethernet0/1)#exit
Device2(config)#interface tentengigabitethernet 0/2
Device2(config-if-tentengigabitethernet0/2)#vsl-channel 1 mode on
Device2(config-if-tentengigabitethernet0/2)#exit
```

### **#Save the configuration on Device2.**

```
Device2#write
Are you sure to overwrite /flash/startup (Yes|No)?y
Building Configuration...done
Write to startup file ... OK
Write to mode file... OK
```

### **#Configure Device1 to run in the stack mode.**

```
Device1#switch mode virtual
This command will convert all interface names to naming convention "interface-type member-number/slot/interface" ,
Please make sure to save current configuration.Do you want to proceed? (yes|no)?y
Converting interface names Building configuration...
Copying the startup configuration to backup file named "startup-backupalone"...
Please wait...system reloading is in progress!
ok
Reset system!
%SYS-5-RELOAD: Reload requested
```

### **#Configure Device2 to run in the stack mode.**

```
Device2#switch mode virtual
This command will convert all interface names to naming convention "interface-type member-number/slot/interface" ,
Please make sure to save current configuration.Do you want to proceed? (yes|no)?y
Converting interface names Building configuration...
Copying the startup configuration to backup file named "startup-backupalone"...
Please wait...system reloading is in progress!
ok
Reset system!
%SYS-5-RELOAD: Reload requested
```

**#Check on Device1, chain stack system has been formed, and Device1 is the master control device of the stack system.**

```
Device1#show switch virtual
```

Codes: L - local-device,I - isolate-device

Virtual Switch Mode : VIRTUAL  
Virtual Switch DomainId : 10  
Virtual Switch mac-address : 0001.7a6a.0255

----- VST MEMBER INFORMATION -----

CODE MemberID Role Pri LocalVsl RemoteVsl

-----  
L 1 Master 255 vsl-channel 1/1 vsl-channel 2/1  
2 Member 200 vsl-channel 2/1 vsl-channel 1/1

Step 2: Configure the basic functions of MVST.

**#Configure the stack system as an MVST management device.**

```
Device1(config)#mvst enable
%MVST-NOTIFY-5: MVST is enabled !
Device1(config)#mvst master
Device1(config)#mvst domain-name test
```

**#Configure stack system link aggregation and start up MVST inspection.**

```
Device1(config)#mvst link-aggregation 1 mode lacp
Device1(config)# mvst interface tengigabitethernet 1/1/1,2/1/1 join link-aggregation 1 active
Device1(config)#interface link-aggregation 1
Device1(config-link-aggregation1)#mvst inspection
Device1(config-link-aggregation1)#exit
Device1(config)#mvst link-aggregation 2 mode lacp
Device1(config)# mvst interface tengigabitethernet 1/1/2,2/1/2 join link-aggregation 2 active
Device1(config)#interface link-aggregation 2
Device1(config-link-aggregation2)#mvst inspection
Device1(config-link-aggregation2)#exit
Device1(config)#mvst link-aggregation 3 mode lacp
Device1(config)# mvst interface tengigabitethernet 1/1/3,2/1/3 join link-aggregation 3 active
Device1(config)#interface link-aggregation 3
Device1(config-link-aggregation3)#mvst inspection
Device1(config-link-aggregation3)#exit
```

**#Enable MVST function on Device3.**

```
Device3#configure terminal
Device3#configure terminal
Device3(config)#mvst enable
%MVST-NOTIFY-5: MVST is enabled !
```

```

Device3(config)#mvst link-aggregation 1 mode lacp
Device3(config)# mvst interface tengigabitethernet 2/1,2/2 join link-aggregation 1 active
Device3(config)#interface link-aggregation 1
Device3(config-link-aggregation1)#mvst inspection
Device3(config-link-aggregation1)#exit

```

%MVST-NOTIFY-5: interface tengigabitethernet2/1 and interface tengigabitethernet2/2 join link-aggregation 1 successfully.

#### #Enable MVST function on Device4.

```

Device4#configure terminal
Device4(config)#mvst enable
%MVST-NOTIFY-5: MVST is enabled !
Device4(config)#mvst link-aggregation 2 mode lacp
Device4(config)# mvst interface tengigabitethernet 2/1,2/2 join link-aggregation 2 active
Device4(config)#interface link-aggregation 2
Device4(config-link-aggregation2)#mvst inspection
Device4(config-link-aggregation2)#exit

```

%MVST-NOTIFY-5: interface tengigabitethernet2/1 and interface tengigabitethernet2/2 join link-aggregation 2 successfully.

#### #Enable MVST function on Device5.

```

Device5#configure terminal
Device5(config)#mvst enable
%MVST-NOTIFY-5: MVST is enabled !
Device5(config)#mvst link-aggregation 3 mode lacp
Device5(config)# mvst interface tengigabitethernet 2/1,2/2 join link-aggregation 3 active
Device5(config)#interface link-aggregation 3
Device5(config-link-aggregation3)#mvst inspection
Device5(config-link-aggregation3)#exit

```

%MVST-NOTIFY-5: interface tengigabitethernet2/1 and interface tengigabitethernet2/2 join link-aggregation 3 successfully.

#Add Device3 as an extension board to the MVST domain, and check the MVST result on Device1 after the device is added.

#Check the MVST result on Device1, you can see that Device3 joins the MVST domain in the form of an extension board, its slot is Slave-slot 0, and its host name changes to switch-ss0.

```

Device1#show mvst topo information

```

```

-----
role    domain-name  interface  mac      device-type  host-name

```

```
-----  
Slave-slot test    link-aggregation 1  0001.7a63.bd76  NSS4330-56TXF(V1)  switch-ss0  
Master test       0001.7a6a.0258  NSS5810-50TXFP(V1)  Device1
```

Step 3: Use Device3 as a template switch and collect the common configuration template.

### #Configure Device3.

```
Device1(config)#configure slave-slot 0  
switch-ss0(config)#snmp-server host 1.1.1.1  
switch-ss0(config)#snmp-server start  
%SNMP-WARMSTART-5 SNMP agent on host switch-ss0 is undergoing a warm start  
switch-ss0(config)#snmp-server enable traps vlan  
switch-ss0(config)#link-aggregation 1  
switch-ss0(config-link-aggregation1)#description management link  
switch-ss0(config-link-aggregation1)#exit  
switch-ss0(config)#vlan 100,200,300
```

### #Check the configuration of the extension board Device3 on Device1.

```
Device1#show running-config slave-slot 0  
hostname switch-ss0  
  
vlan 100,200,300  
link-aggregation 1  
description management link  
no spanning-tree enable  
mvst inspection  
exit  
  
snmp-server start  
snmp-server view default 1.2 include  
snmp-server view default 1.0.8802 include  
snmp-server view default 1.1.2 include  
snmp-server view default 1.3.111 include  
snmp-server view default 1.3.6.1 include  
snmp-server community public view default ro  
snmp-server enable traps vlan  
snmp-server host 1.1.1.1 traps community public version 2
```

### #Save the configuration of Device3 on Device1.

```
Device1#write slave-slot 0  
Are you sure to overwrite slave slot 0 /flash/startup (Yes|No)?y  
Device1#
```

Jan 9 2015 16:32:34: %MVST-WRITE\_RESULT-5: The slave slot 0 write to startup file successfully.

Step 4: Automatically issue the configuration of Device3 as a common configuration template.

**#Configure common configuration auto issue on Device1**

```
Device1(config)#mvst configure template slave-slot 0
Are you sure to overwrite configure template /flash/mvst-template (Yes|No)?y
Get the slave slot 0 startup-config...OK
Write to /flash/mvst-template ....OK.
Device1(config)#
```

Step 5: Add the extension board to the MVST domain to automatically load the configuration template.

**#Connect the extension boards Device4 and Device5 to the MVST domain, you can see on Device1 the print information automatically issued by the configuration template.**

```
Device1#
%MVST-Slave_slot_add-5:Slave slot 1 add to the MVST
%MVST-Slave_slot_add-5:Slave slot 2 add to the MVST.
%MVST-EXECUTE_COFNIG-5:Slave slot 1 is going to execute configure template /flash/mvst-template.
%MVST-EXECUTE_COFNIG-5:Slave slot 1 execute configure file successfully!
%MVST-EXECUTE_COFNIG-5:Slave slot 2 is going to execute configure template /flash/mvst-template.
%MVST-EXECUTE_COFNIG-5:Slave slot 2 execute configure file successfully!
```

**#Check the MVST result on Device1. By default, the host names of Device4 and Device5 have the suffixes ss1 and ss2 added as switch-ss1 and switch-ss2 respectively.**

```
Device1#show mvst topo information
```

```
-----
role    domain-name  interface    mac          device-type  host-name
-----
Slave-slot test    link-aggregation 1 0001.7a63.bd76 NSS4330-56TXF(V1)  switch-ss0
Slave-slot test    link-aggregation 2 0001.7a64.72aa NSS4330-56TXF(V1)  switch-ss1
Slave-slot test    link-aggregation 3 0001.7a63.bd43 NSS4330-56TXF(V1)  switch-ss2
Master test        0001.7a6a.0258 NSS5810-50TXFP(V1) Device1
```

**#Check the configuration of Device4 on Device1, the configuration is successfully issued.**

```
Device1#show running-config slave-slot 1
hostname switch-ss1

vlan 100,200,300

link-aggregation 1
description management link
```

```
no spanning-tree enable
mvst inspection
exit
```

```
snmp-server start
snmp-server view default 1.2 include
snmp-server view default 1.0.8802 include
snmp-server view default 1.1.2 include
snmp-server view default 1.3.111 include
snmp-server view default 1.3.6.1 include
snmp-server community public view default ro
snmp-server enable traps vlan
snmp-server host 1.1.1.1 traps community public version 2
```

**#Check the configuration of Device5 on Device1, the configuration is successfully issued.**

```
Device1#show running-config slave-slot 2
hostname switch-ss2
```

```
vlan 100,200,300
```

```
link-aggregation 1
description management link
no spanning-tree enable
mvst inspection
exit
```

```
snmp-server start
snmp-server view default 1.2 include
snmp-server view default 1.0.8802 include
snmp-server view default 1.1.2 include
snmp-server view default 1.3.111 include
snmp-server view default 1.3.6.1 include
snmp-server community public view default ro
snmp-server enable traps vlan
snmp-server host 1.1.1.1 traps community public version 2
```

**Step 6: Forcibly issue the common configuration template.**

**#Modify the configuration of Device3 and add ACL configuration.**

```
Device1(config)#configure slave-slot 0
switch-ss0(config)#ip access-list extended test
```

```
switch-ss0(config-ext-nacl)#permit ip 192.168.0.1 0.0.0.255 any
switch-ss0(config-ext-nacl)#permit ip any any
switch-ss0(config-ext-nacl)#exit
switch-ss0(config)#end
switch-ss0#show access-list
ip access-list extended test
10 permit ip 192.168.0.0 0.0.0.255 any
20 permit ip any any
```

#### #Save the configuration of Device3 on Device1.

```
Device1#write slave-slot 0
Are you sure to overwrite slave slot 0 /flash/startup (Yes|No)?y
Device1#
%MVST-WRITE_RESULT-5: The slave slot 0 write to startup file successfully.
%MVST-COLLECT_STARTUP-5: Collect slave slot 0 startup begin.
%MVST-COLLECT_STARTUP-5: Collect slave slot 0 startup OK.
```

#### #Recollect startup of Device3 on Device1 as a new common configuration template.

```
Device1(config)#mvst configure template slave-slot 0
Are you sure to overwrite configure template /flash/mvst-template (Yes|No)?y
Get the slave slot 0 startup-config...OK
Write to /flash/mvst-template ....OK.
```

#### #Forcibly issue the common configuration template on Device1 to Device4. Information for successful issue is displayed.

```
Device1(config)#mvst apply configure template slave-slot 1
%MVST-EXECUTE_COFNIG-5: Slave slot 1 is going to execute configure template /flash/ mvst-template
%MVST-EXECUTE_COFNIG-5: Slave slot 1 execute configure file successfully!
```

#### #Check that the configuration of Device4 contains the latest ACL configuration.

```
Device1(config)#configure slave-slot 1
switch-ss1#show access-list
ip access-list extended test
10 permit ip 192.168.0.0 0.0.0.255 any
20 permit ip any any
```

### 123.3.3 Configure Auto Issue of Binding Configuration

#### Network Requirements

- Device1 and Device2 form a stack system as MVST management device, Device3, Device4, and Device5 are used as extension boards, and the last two ports of the extension boards

are connected to the MVST management device;

- Perform differentiated configuration for Device3, Device4, and Device5, and bind configurations of the extension boards corresponding to link aggregation 1, link aggregation 2, and link aggregation 3 to the MVST management device;
- Simulating replacement with a brand new device Device6 after the failure of Device3, with the MVST management device capable of automatically issuing the previously collected configuration of Device3.
- Simulating that when link aggregation 1 of the MVST management device fails, link aggregation 4 needs to be created, and the configuration of Device3 bound to link aggregation group 1 is transitioned to link aggregation 4.

### Network Topology

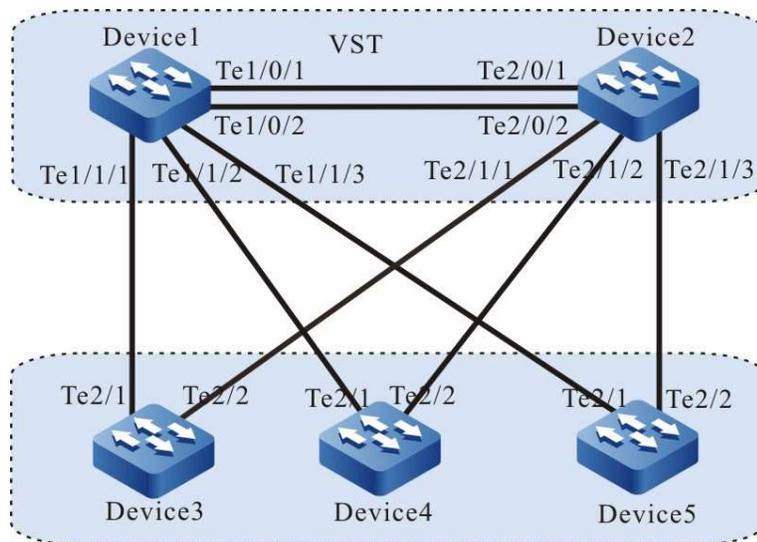


Figure 123-4 Configuring Auto Issue of Binding Configuration

### Configuration Steps

Step 1: Configure the VST system.

#On Device1, configure the virtual switch member device ID as 1, and configure the domain ID as 10 and the priority as 255.

```
Device1#configure terminal
Device1(config)#switch virtual member 1
Do you want to modify member id(Yes|No)?y
% Member ID 1 config will take effect only after the exec command 'switch mode virtual' is issued
Device1(config-vst-member-1)#domain 10
% Domain ID 10 config will take effect only after the exec command 'switch mode virtual' is issued
Device1(config-vst-member-1)#priority 255
Device1(config-vst-member-1)#exit
```

**#On Device1, create virtual switch link interface 1, and add ports tengigabitethernet0/1 and tengigabitethernet0/2 to the virtual switch link interface 1.**

```
Device1(config)#vsl-channel 1
Device1(config-vsl-channel-1)#exit
Device1(config)#interface tengigabitethernet 0/1
Device1(config-if-tengigabitethernet0/1)#vsl-channel 1 mode on
Device1(config-if-tengigabitethernet0/1)#exit
Device1(config)#interface tengigabitethernet 0/2
Device1(config-if-tengigabitethernet0/2)#vsl-channel 1 mode on
Device1(config-if-tengigabitethernet0/2)#exit
```

**#Save the configuration on Device1.**

```
Device1#write
Are you sure to overwrite /flash/startup (Yes|No)?y
Building Configuration...done
Write to startup file ... OK
Write to mode file... OK
```

**#On Device2, configure the virtual switch member device ID as 1, and configure the domain ID as 10 and the priority as 200.**

```
Device2#configure terminal
Device2(config)#switch virtual member 2
Do you want to modify member id(Yes|No)?y
% Member ID 2 config will take effect only after the exec command 'switch mode virtual' is issued
Device2(config-vst-member-2)#domain 10
% Domain ID 10 config will take effect only after the exec command 'switch mode virtual' is issued
Device2(config-vst-member-2)#priority 200
Device2(config-vst-member-2)#exit
```

**#On Device2, create virtual switch link interface 1, and add ports tengigabitethernet1/1 to the virtual switch link interface 1.**

```
Device2(config)#vsl-channel 1
Device2(config-vsl-channel-1)#exit
Device2(config)#interface tengigabitethernet 0/1
Device2(config-if-tengigabitethernet0/1)#vsl-channel 1 mode on
Device2(config-if-tengigabitethernet0/1)#exit
Device2(config)#interface tengigabitethernet 0/2
Device2(config-if-tengigabitethernet0/2)#vsl-channel 1 mode on
Device2(config-if-tengigabitethernet0/2)#exit
```

**#Save the configuration on Device2.**

```
Device2#write
Are you sure to overwrite /flash/startup (Yes|No)?y
Building Configuration...done
Write to startup file ... OK
Write to mode file... OK
```

### #Configure Device1 to run in the stack mode.

```
Device1#switch mode virtual
This command will convert all interface names to naming convention "interface-type member-number/slot/interface" ,
Please make sure to save current configuration.Do you want to proceed? (yes|no)?y
Converting interface names Building configuration...
Copying the startup configuration to backup file named "startup-backupalone"...
Please wait...system reloading is in progress!
ok
Reset system!
%SYS-5-RELOAD: Reload requested
```

### #Configure Device2 to run in the stack mode.

```
Device2#switch mode virtual
This command will convert all interface names to naming convention "interface-type member-number/slot/interface" ,
Please make sure to save current configuration.Do you want to proceed? (yes|no)?y
Converting interface names Building configuration...
Copying the startup configuration to backup file named "startup-backupalone"...
Please wait...system reloading is in progress!
ok
Reset system!
%SYS-5-RELOAD: Reload requested
```

### #Check on Device1, chain stack system has been formed, and Device1 is the master control device of the stack system.

```
Device1#show switch virtual
Codes: L - local-device,I - isolate-device
```

```
Virtual Switch Mode      : VIRTUAL
Virtual Switch DomainId  : 10
Virtual Switch mac-address : 0001.7a6a.0255
```

```
----- VST MEMBER INFORMATION -----
CODE MemberID Role  Pri LocalVsl  RemoteVsl
-----
L 1 Master 255 vsl-channel 1/1 vsl-channel 2/1
 2 Member 200 vsl-channel 2/1 vsl-channel 1/1
```

Step 2: Configure the basic functions of MVST.

**#Configure the stack system as an MVST management device.**

```
Device1(config)#mvst enable
%MVST-NOTIFY-5: MVST is enabled !
Device1(config)#mvst master
Device1(config)#mvst domain-name test
```

**#Configure stack system link aggregation and start up MVST inspection.**

```
Device1(config)#mvst link-aggregation 1 mode lacp
Device1(config)# mvst interface tengigabitethernet 1/1/1,2/1/1 join link-aggregation 1 active
Device1(config)#interface link-aggregation 1
Device1(config-link-aggregation1)#mvst inspection
Device1(config-link-aggregation1)#exit
Device1(config)#mvst link-aggregation 2 mode lacp
Device1(config)# mvst interface tengigabitethernet 1/1/2,2/1/2 join link-aggregation 2 active
Device1(config)#interface link-aggregation 2
Device1(config-link-aggregation2)#mvst inspection
Device1(config-link-aggregation2)#exit
Device1(config)#mvst link-aggregation 3 mode lacp
Device1(config)# mvst interface tengigabitethernet 1/1/3,2/1/3 join link-aggregation 3 active
Device1(config)#interface link-aggregation 3
Device1(config-link-aggregation3)#mvst inspection
Device1(config-link-aggregation3)#exit
```

**#Enable MVST function on Device3.**

```
Device3#configure terminal
Device3#configure terminal
Device3(config)#mvst enable
%MVST-NOTIFY-5: MVST is enabled !
Device3(config)#mvst link-aggregation 1 mode lacp
Device3(config)# mvst interface tengigabitethernet 2/1,2/2 join link-aggregation 1 active
Device3(config)#interface link-aggregation 1
Device3(config-link-aggregation1)#mvst inspection
Device3(config-link-aggregation1)#exit
```

%MVST-NOTIFY-5: interface tengigabitethernet2/1 and interface tengigabitethernet2/2 join link-aggregation 1 successfully.

**#Enable MVST function on Device4.**

```
Device4#configure terminal
Device4(config)#mvst enable
```

%MVST-NOTIFY-5: MVST is enabled !

Device4(config)#mvst link-aggregation 2 mode lacp

Device4(config)# mvst interface tengigabitethernet 2/1,2/2 join link-aggregation 2 active

Device4(config)#interface link-aggregation 2

Device4(config-link-aggregation2)#mvst inspection

Device4(config-link-aggregation2)#exit

%MVST-NOTIFY-5: interface tengigabitethernet2/1 and interface tengigabitethernet2/2 join link-aggregation 2 successfully.

### #Enable MVST function on Device5.

Device5#configure terminal

Device5(config)#mvst enable

%MVST-NOTIFY-5: MVST is enabled !

Device5(config)#mvst link-aggregation 3 mode lacp

Device5(config)# mvst interface tengigabitethernet 2/1,2/2 join link-aggregation 3 active

Device5(config)#interface link-aggregation 3

Device5(config-link-aggregation3)#mvst inspection

Device5(config-link-aggregation3)#exit

%MVST-NOTIFY-5: interface tengigabitethernet2/1 and interface tengigabitethernet2/2 join link-aggregation 3 successfully.

### #Connect Device3, Device4, and Device5 to the MVST domain in turn, and check the MVST result after the devices are connected.

#Check the MVST result on Device1, you can see that Device3, Device4, and Device5 are added to the MVST domain in the form of extension boards. The slots are Slave-slot0, Slave-slot1, and Slave-slot2, and their host names change to switch-ss0, switch-ss1, switch-ss2.

Device1#show mvst topo information

```
-----  
role  domain-name  interface  mac          device-type  host-name  
-----  
Slave-slot test    link-aggregation 1  0001.7a63.bd76  NSS4330-56TXF(V1)  switch-ss0  
Slave-slot test    link-aggregation 2  0001.7a64.72aa  NSS4330-56TXF(V1)  switch-ss1  
Slave-slot test    link-aggregation 3  0001.7a63.bd43  NSS4330-56TXF(V1)  switch-ss2  
Master   test           0001.7a6a.0258  NSS5810-50TXFP(V1)  Device1
```

Step 3: Configure the function of auto issue of binding configuration.

### #Perform differentiated configuration on Device3, Device4, and Device5.

Device1(config)#configure slave-slot 0

switch-ss0(config)#vlan 100

```
switch-ss0(config)#exit
switch-ss0#exit
switch-ss0>exit
Device1(config)#configure slave-slot 1
switch-ss1(config)#vlan 200
switch-ss1(config)#exit
switch-ss1#exit
switch-ss1>exit
Device1(config)#configure slave-slot 2
switch-ss2(config)#vlan 300
switch-ss2(config)#exit
switch-ss2#exit
switch-ss2>exit
```

**#Save the configurations of Device3, Device4, and Device5 on Device1.**

```
Device1#write slave-slot 0
Are you sure to overwrite slave slot 0 /flash/startup (Yes|No)?y
Device1#
Jan 9 2015 16:32:34: %MVST-WRITE_RESULT-5: The slave slot 0 write to startup file successfully.
Device1#write slave-slot 1
Are you sure to overwrite slave slot 0 /flash/startup (Yes|No)?y
Device1#
Jan 9 2015 16:32:34: %MVST-WRITE_RESULT-5: The slave slot 1 write to startup file successfully.
Device1#write slave-slot 2
Are you sure to overwrite slave slot 0 /flash/startup (Yes|No)?y
Device1#
Jan 9 2015 16:32:34: %MVST-WRITE_RESULT-5: The slave slot 2 write to startup file successfully.
```

**#Configure the function of auto issue of binding configuration on Device1, and collect to the MVST management device, startup of the extension boards corresponding to link aggregation group 1, link aggregation group 2, and link aggregation group 3.**

```
Device1(config)#mvst bind startup link-aggregation 1
Device1(config)#
Jan 9 2015 15:25:16: %MVST-COLLECT_STARTUP-5: Collect slave slot 0 startup begin.
Jan 9 2015 15:25:16: %MVST-COLLECT_STARTUP-5: Collect slave slot 0 startup OK.
Device1(config)#mvst bind startup link-aggregation 2
Device1(config)#
Jan 9 2015 15:25:16: %MVST-COLLECT_STARTUP-5: Collect slave slot 1 startup begin.
Jan 9 2015 15:25:16: %MVST-COLLECT_STARTUP-5: Collect slave slot 1 startup OK.
Device1(config)#mvst bind startup link-aggregation 3
Device1(config)#
```

Jan 9 2015 15:25:16: %MVST-COLLECT\_STARTUP-5: Collect slave slot 2 startup begin.

Jan 9 2015 15:25:16: %MVST-COLLECT\_STARTUP-5: Collect slave slot 2 startup OK.

**#Check the result of auto issue of binding configuration on Device1. Startups numbered extension board 0, 1, and 2 are collected into the startup-lag1, startup-lag2, and startup-lag3 files in the USB.**

Device1#show mvst startup bind info

```
-----  
Interface      Bind-file-name  
-----  
link-aggregation 1  /usb/startup-lag1  
link-aggregation 2  /usb/startup-lag2  
link-aggregation 3  /usb/startup-lag3
```

**#After enabling the MVST function for a brand new device Device6, join the link aggregation group 1 of the MVST management device to the MVST domain to replace Device3. Device6 is added to the MVST domain in the form of an extension board, and its slot is Slave-slot3. The print information about the configuration of auto issue startup- LAG1 is displayed.**

Device1#

Jan 9 2015 16:54:46: %MVST-Slave\_slot\_add-5:Slave slot 3 add to the MVST.

Jan 9 2015 16:54:47: %MVST-EXECUTE\_COFNIG-5: Slave slot 3 is going to execute configure file /usb/startup-lag1.

Jan 9 2015 16:54:48: %MVST-EXECUTE\_COFNIG-5: Slave slot 3 execute configure file successfully!

**#Check the MVST result on Device1. Device6 joins the MVST domain in the form of an extension board. Its slot is Slave-slot3 and its host name changes to switch-ss3.**

Device1#show mvst topo information

```
-----  
role   domain-name  interface  mac          device-type  host-name  
-----  
Slave-slot test  link-aggregation 4  0001.7a63.bd89  NSS4330-56TXF(V1)  switch-ss3  
Slave-slot test  link-aggregation 2  0001.7a64.72aa  NSS4330-56TXF(V1)  switch-ss1  
Slave-slot test  link-aggregation 3  0001.7a63.bd43  NSS4330-56TXF(V1)  switch-ss2  
Master   test          0001.7a6a.0258  NSS5810-50TXFP(V1)  Device1
```

**#Check the configuration of Device6. Device6 has loaded the configuration of Device3, and VLAN100 has been created.**

Device1#show run slave-slot 3

vlan 100

**Step 3: Configure the function of transitioning auto issue of binding configuration.**

**#Configure link aggregation 4 on Device1**

Device1(config)#interface tengigabitethernet 1/1/1,2/1/1

```
Device1(config-if-range)#link-aggregation 4 active
```

```
Device1(config-if-range)#exit
```

#Configure transitioning of auto issue of binding configuration on Device1, and transition the original configuration collected by link aggregation 1 to link aggregation 4.

```
Device1(config)#mvst bind startup link-aggregation 4
```

```
Device1(config)#mvst relocate configure interface link-aggregation 1 interface link-aggregation 4
```

```
interfaceinterface link-aggregation1 file will cover interface link-aggregation4 file, are you sure to do it(Yes|No)?y
```

#Check on Device1 that the configuration migration is successful, and there is a configuration file named startup-lag4 in the USB.

```
Device1(config-fs)#cd /usb
```

```
Device1(config-fs)#dir
```

```
7256      JAN-09-2015 17:58:16  startup-lag4
```

#Delete startup of Device6 and reboot Device6 without saving the configuration. After the device is started, you can see on Device1 that Device6 has loaded the configuration of startup-lag4, which is consistent with the startup-lag1 configuration before the transition.

```
Device1#show run slave-slot 3
```

```
vlan 100
```

# 124 VD

---

## 124.1 Overview

VD (Virtual Device) is virtual device technology, which is a complete 1:N virtualization technology (the virtualization technology includes two types: N:1 virtualization means that multiple physical devices are virtualized into one logical device; 1:N virtualization means that one physical device is virtualized into multiple logical devices). From the software point of view, it completely virtualizes the data plane, control plane, and management plane of the network operating system. Each user mode process starts and runs independently in the VD. Although every VD shares one kernel, the data between the VDs in the kernel is also separate. In terms of hardware, not only monoboard is used as independent logical device, but also the storage space occupied

by each VD, the available CPU and other resources are also divided. VD is made very close to a single physical device. VD has complete device functions, independent software environment and data, and independent hardware resources. One VD can even be rebooted alone like one physical device without affecting the normal running of other VDs on the physical device.

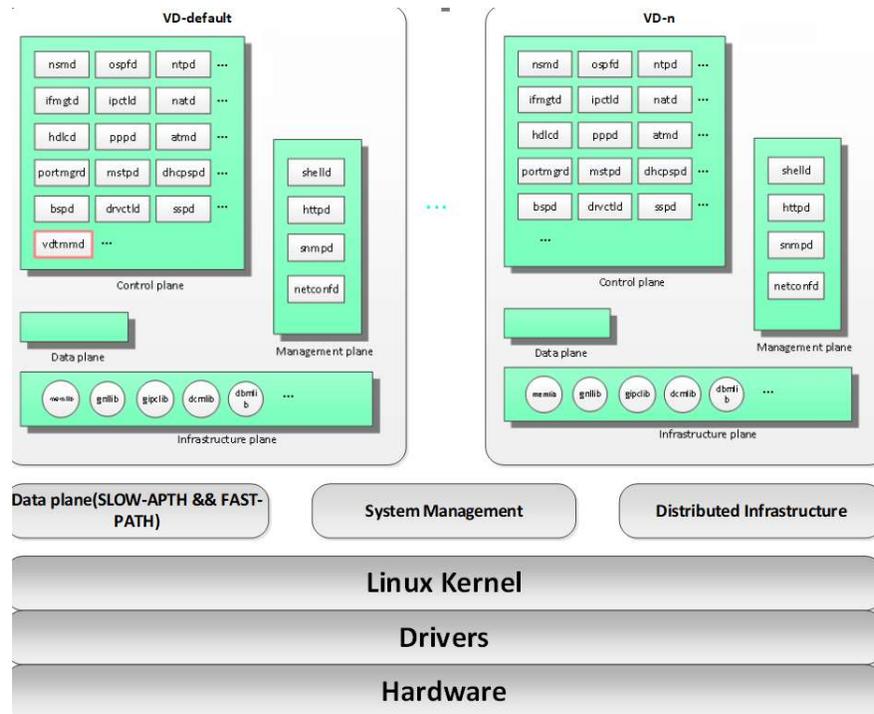


Figure 123-17 Frame Diagram of VD Technology

## 124.2 VD Function Configuration

### 124.2.1 Configure VD

By default, the device has a built-in default virtual machine VDO, called default virtual machine (host machine). All board resources belong to VDO by default, and VDO cannot be created or deleted.

#### Configuration Condition

None

#### Configure VD

VD is an entity run by a service unit and needs to be created manually.

Table 123-18 Configuring VD

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Create VD	<b>virtual-device</b> <i>vd-id</i>	Mandatory By default, VD0 is created by default
Assign Lpu board resources	<b>assign lpu</b> <i>&lt;slotId&gt;</i>	Mandatory By default, the manually created VD does not contain any LPU board resources
Configure the upper limit of VD memory	<b>resource memory upper-limit-in-mega</b> <i>number</i>	Optional By default, 660M memory is assigned for each VD
Configure description information	<b>description</b> <i>string</i>	Optional By default, there is no description information
Start VD	<b>virtual-device start</b>	Mandatory By default, VD is not started

### 124.2.2 Log in to VD

After VD is configured, you can log in to VD to perform service configuration. To log in to VD, you must ensure that VD has been started.

#### Configuration Condition

None

#### Log in to VD

When VD is activated, VD will start, and you can log in to VD after the start is complete

Table 123-19 Logging in to VD

Step	Command	Description
Enter the privilege configuration mode	<b>enable</b>	-
Log in to VD	<b>switch to virtual-device <i>vd- id</i> [force]</b>	Mandatory Force means mandatory login. When someone else occupies the serial port of this VD, use compulsory means.

### 124.2.3VD Monitoring and Maintaining

Table 123-20 VD Monitoring and Maintaining

Command	Description
<b>show virtual-device summary</b>	Show summary information of all VDs
<b>show virtual-device verbose [vd- id ]</b>	Show detailed information of the specified VD or all VDs
<b>show system virtual-device lpu list</b>	Show information about lpu in place in VD
<b>show virtual-device <i>vd-id</i> console log</b>	Show log information of the specified VD

## 124.3 Typical Configuration Example of VD

### Networking Requirements

- Isolate user groups, and divide different user groups into different virtual devices to realize network service flow isolation and fault isolation, and ensure reliability and safety requirements.

- As shown in Figure 123-5, the office area and the production area are divided to different VDTs according to service parts.

### Network Topology

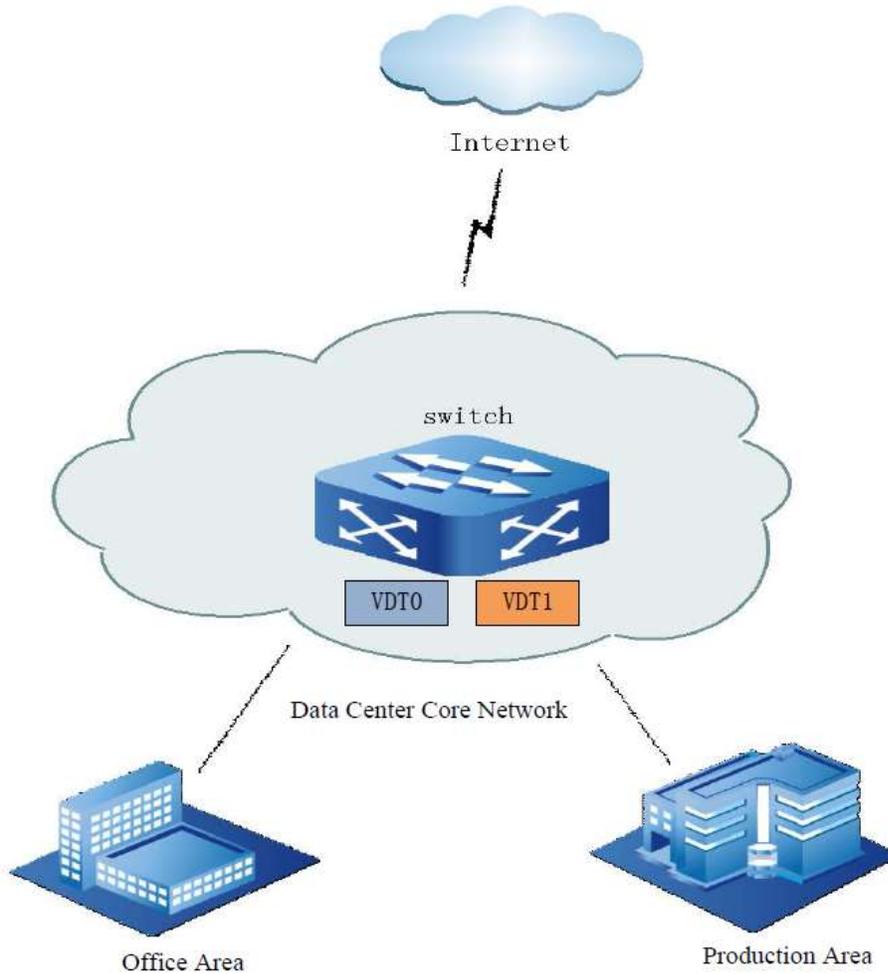


Figure 123-6 : VDT Network Topology

### Configuration Steps

Step 1: Configure VDT

#Create virtual machine vdt1 on Switch, assign LPU6 to vdt1, and activate the virtual machine

switch#conf terminal

```
switch(config)#virtual-device vdt1
switch(config-vd-1)#assign lpu 6
Please save the configuration after executing the allocation command!
This LPU will be assigned, are you sure?(yes/no)y
switch(config-vd-1)#description vdt1
switch(config-vd-1)#virtual-device start
start:ok.
switch(config-vd-1)#exit
switch(config)#
```

Step 2:        Log in to VDT.

#Log in to the corresponding virtual machine configuration service, with service configuration omitted.

```
switch#switch to virtual-device vdt1
vdt1>enable
vdt1#
```

# 125 TRILL

---

## 125.1 Overview

TRILL (TRansparent Interconnection of Lots of Links) uses three-layer routing technology to construct a two-layer switching network. It has the following technical features:

1. TRILL data frames are sent hop by hop within the network according to the routing mode, and there is no need to block some ports like the spanning tree protocol, so it can make full use of ports and bandwidth resources.

2. The Spanning Tree Protocol limits the diameter of two-layer network under normal circumstances to not exceed 7, but TRILL technology has no such limitation, so TRILL is more in line with the need for building a large two-layer network.

Although the three-layer routing technology is adopted, the TRILL network is still a two-layer switching network to the outside, that is, the TRILL technology still retains the simplicity and flexibility of the two-layer switching network, which facilitates the migration of data center servers and virtual machines.

### 125.1.1 Basic Concepts

- RB

RB refers to Routing Bridge that is a switch running TRILL protocol. It can be divided into Edge RB and Transit RB according to its position in the TRILL network. Edge RB is located at the edge of the TRILL network, with Access ports and Trunk/P2P ports on it; Transit RB is located inside the TRILL network, with no Access ports but Trunk/P2P ports on it.

- system id

Each RB has a unique identifier in the TRILL network, that is, the system ID of this RB, the length is fixedly 6 bytes, and the format is similar to that of MAC address.

- nickname

Each RB has a network address in the TRILL network, that is, the nickname of this RB, the length is fixedly 2 bytes, and its function is equivalent to the IP address in the IP network.

- Port Type

There are three types of TRILL port:

1. Access type: The access port of the TRILL network. This type of port can only send and receive raw Ethernet frames, but cannot send and receive TRILL data frames.

2. Trunk type: The internal port of the TRILL network. This type of port cannot send and receive raw Ethernet frames, but can only send and receive TRILL data frames.

3. P2P type: The internal port of the TRILL network. This type of port cannot send and receive raw Ethernet frames, but can only send and receive TRILL data frames. The difference between the P2P type and the Trunk type is the fact that the P2P type port involves no concept of DRB and does not carry out DRB resolution, while the Trunk type port needs to carry out DRB resolution.

If all neighbor ports on one link are of Access type or Trunk type, then this link is called broadcast link; if two neighbor ports on one link are of P2P type, then this link is called point-to-point link.

- DRB

DRB refers to Designated Routing Bridge. In the broadcast link, two or more RBs that are neighbors to each other will resolve one RB as DRB, and the DRB is responsible for assigning AVF for VLANs on these RBs.

- AVF

AVF refers to Appointed VLAN-x Forwarder. When certain broadcast link is connected to the TRILL network via two or more Edge RBs, for traffic of certain VLAN, only one Edge RB can enter and exit the TRILL network in order to prevent loops. This RB is called AVF of this VLAN.

- Designated VLAN

In the TRILL network, TRILL data frames are transmitted via designated VLAN (abbreviated as DVLAN). In addition, the designated VLAN is also used to transmit some TRILL protocol packets (such as LSP packets, CSNP/PSNP packets, and some Hello packets).

- LSP

LSP refers to Link State Protocol Data Unit. Each RB has its own LSP, which describes the state of the link between this RB and each neighbor RB.

- LSPDB

LSPDB refers to Link State Protocol DataBase which is composed of LSPs of all RBs in the TRILL network.

## 125.1.2 TRILL Frame Format

TRILL frames include two types: TRILL data frames and TRILL protocol frames, which are introduced separately below.

- TRILL Data Frame

The TRILL data frame is formed by adding TRILL header in front of raw Ethernet frame, and then encapsulating with outer Ethernet header. The format of the TRILL data frame is shown in the figure below.

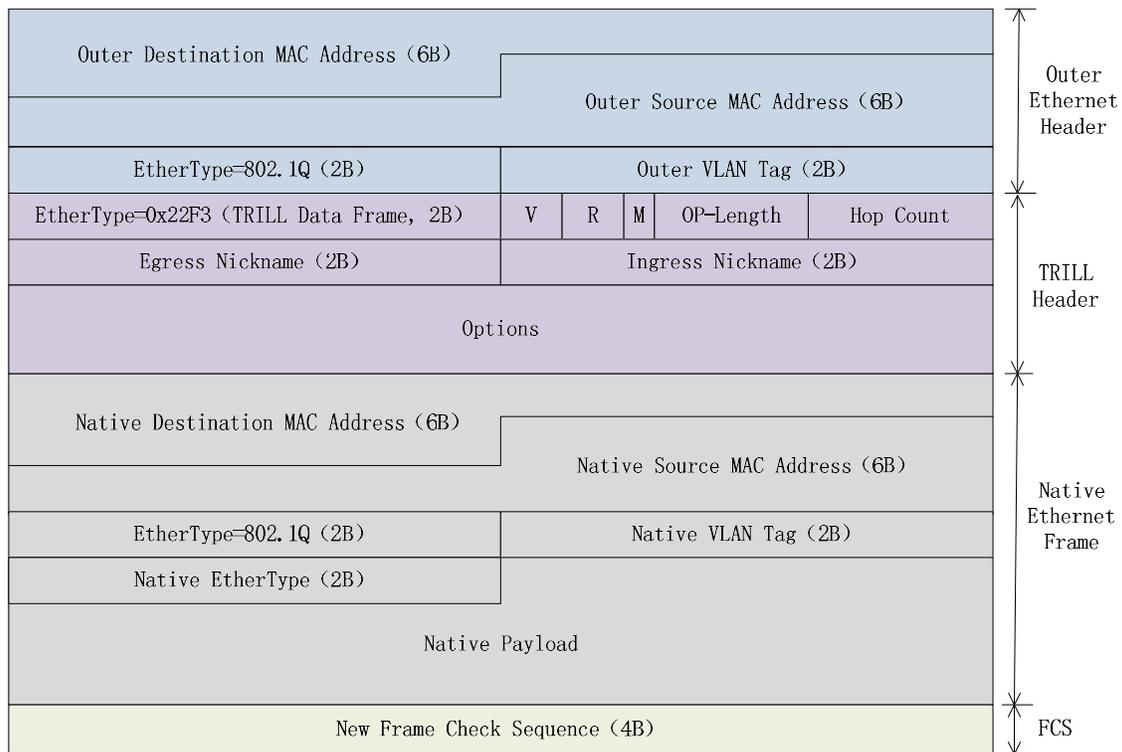


Figure 125-1 TRILL Data Frame Format

The meanings of the fields in the TRILL Header are explained as follows:

- ✧ EtherType: Ethernet type is fixedly 0x22F3, which represents TRILL data frame.
- ✧ V: Version number, currently 0.
- ✧ R: Reserved bit for future extension.
- ✧ M: Identifies whether one packet is multicast packet. 0 indicates that this packet is known unicast message, and 1 indicates that this packet is multicast packet. Since multicast, broadcast, and unknown unicast packets have the same forwarding mechanism in the TRILL network, these three types of packets are collectively referred to as multicast packets.
- ✧ OP-Length: Length of the Options field. 0 indicates that here is no Options field.
- ✧ Hop Count: Used to prevent loops. It is reduced by 1 for each hop in the TRILL network. When the hop count is 0, the RB will discard the packet.
- ✧ Egress Nickname: When M is 0, this field is the nickname of egress RB; when M is 1, this field is the nickname of the root RB of the distribution tree.
- ✧ Ingress Nickname: The nickname of the ingress RB.
- ✧ Options: TRILL header option field. This field will only be present when Op-Length is not 0.

The meanings of the fields of the Outer Ethernet Header are explained as follows:

- ✧ Outer Destination MAC Address: When M is 0, this field is the MAC address of the next hop RB; when M is 1, this field is fixedly 01-80-C2-00-00-40.
- ✧ Outer Source MAC Address: The MAC address of the RB itself that forwards the packet.
- ✧ Outer VLAN Tag: The designated VLAN of the TRILL port that forwards the packet.

- TRILL Protocol Frame

Each RB in the TRILL network needs to run the TRILL protocol and exchange TRILL protocol frames. The format of the TRILL protocol frame is shown in the figure below.

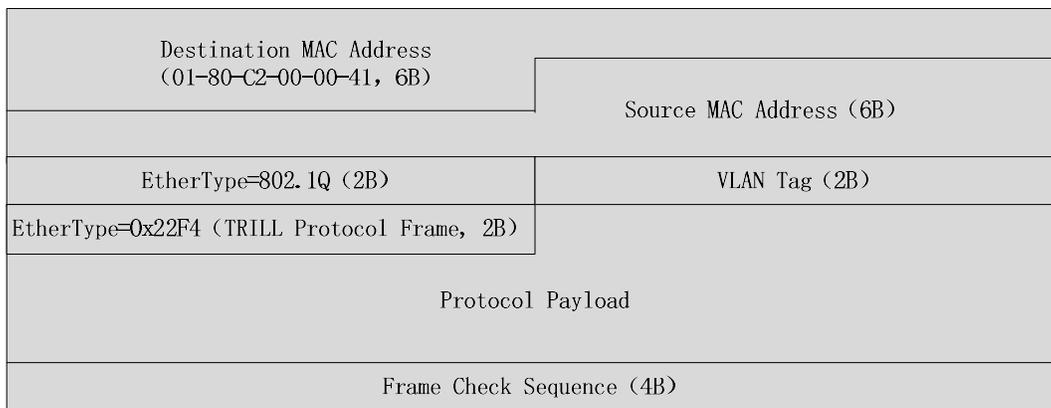


Figure 125-2 TRILL Protocol Frame Format

The meanings of some fields in the TRILL protocol frame are explained as follows:

- ✧ Destination MAC Address: fixedly 01-80-C2-00-00-41 (this multicast address is called All-IS-IS-RBridges).
- ✧ Source MAC Address: The source MAC address of the RB that sends this protocol frame.
- ✧ VLAN Tag: The VLAN that transmits the protocol frame. In most cases, this VLAN corresponds to the designated VLAN of the sending port, but for some Hello messages, this VLAN corresponds to the Announcing VLAN of the sending port.
- ✧ EtherType: Ethernet type is fixedly 0x22F4, which represents TRILL protocol frame.
- ✧ Protocol Payload: TRILL protocol packet payload, namely TRILL PDU.

### 125.1.3 TRILL Forwarding Mechanism

How the TRILL data frame is forwarded in the TRILL network is described in two cases: unicast data frame and multicast data frame.

- TRILL Unicast Data Frame Forwarding

The TRILL network in the figure below contains five RBs. Among them, RB1, RB4, and RB5 are located at the edge of the TRILL network (used as Edge RBs), RB2 and RB3 are located inside the TRILL network (used as transit RBs), and HostA and HostB are connected via the TRILL network. How the known unicast frames from HostA to HostB are forwarded over the TRILL network is analyzed below.

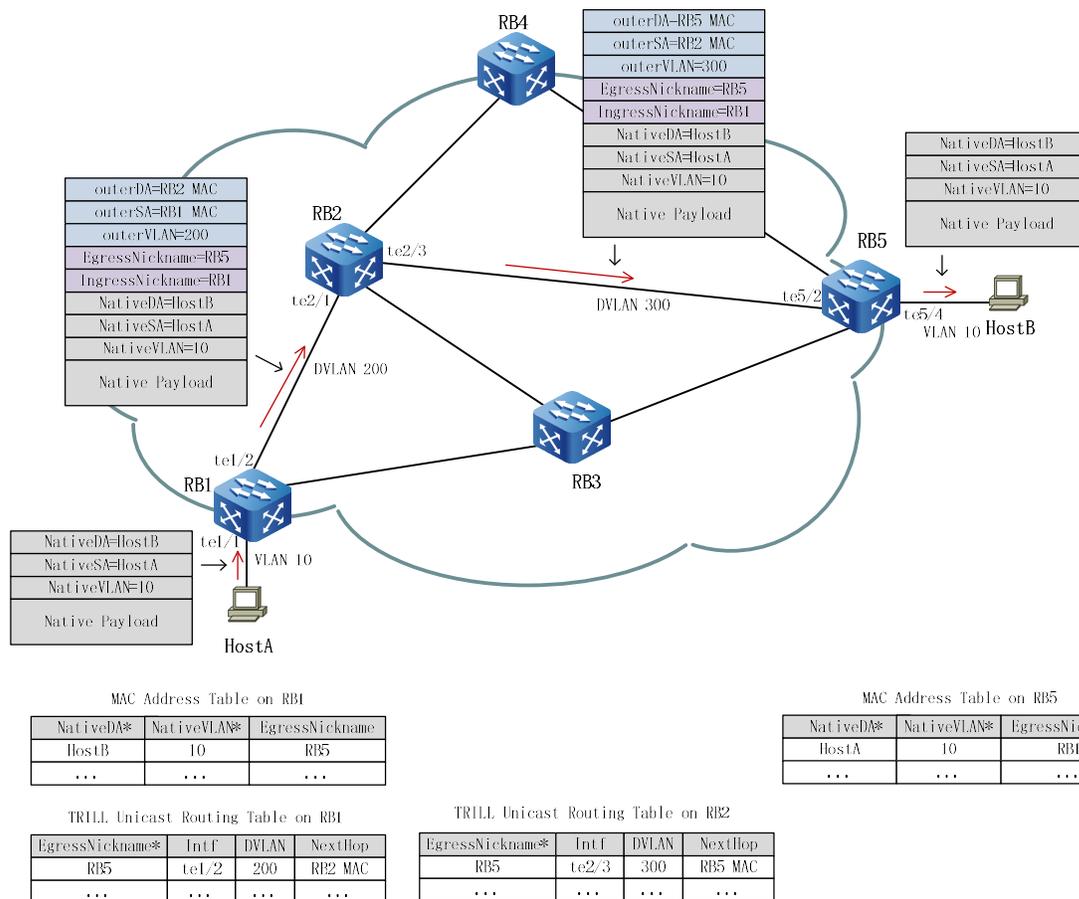


Figure 125-3 Example of TRILL Unicast Frame Forwarding Process

Take RB1 as an example. There are two tables in it (the search key of the tables is identified by \*). One table is the MAC address table, which can learn the MAC address and VLAN of HostB from the packet sent by the remote HostB, as well as the nickname of RB5 directly connected to HostB. The other table is the TRILL unicast routing table, which is calculated by the TRILL protocol. It records, from native RB (that is, RB1) to each other RB in the TRILL network, from which port should forwarding be carried out, how much outer VLAN should be encapsulated, and what MAC of next hop is.

When RB1 receives the raw Ethernet frame sent from HostA to HostB, it uses the destination MAC address and VLAN of the raw Ethernet frame to check the MAC address table, and learns that the packet should be sent to RB5. Then it uses the nickname of RB5 to check the TRILL unicast routing table, and learns that the outer Ethernet header of the packet should be encapsulated with outerVLAN as 200.

OuterDA is MAC of the next-hop neighbor RB2, outerSA is RB1's own MAC, and IngressNickname of the TRILL header is RB1's own nickname, and EgressNickname is the nickname of the destination RB5. After the TRILL frame is encapsulated, it is forwarded from te1/2 of RB1.

After RB2 receives the TRILL data frame sent by RB1, it uses EgressNickname in the TRILL header (namely, the nickname of RB5) to check its TRILL unicast routing table, and learns that the outerVLAN encapsulating the outer Ethernet header of the packet should be changed to 300. OuterDA is MAC of the next-hop neighbor RB5, outerSA is RB2's own MAC, IngressNickname and EgressNickname in the TRILL header remain unchanged, and only the hop count is reduced by 1. After the encapsulation to the TRILL frame is changed, it is forwarded from te2/3 of RB2.

Because RB5 is located at the edge of the TRILL network, after RB5 receives the TRILL data frame sent by RB2, it must first learn the remote source MAC address, and learn the MAC address and VLAN of HostA, and IngressNickname (i.e. RB1) to the MAC address table of RB5. Then it resolves the TRILL header and finds that EgressNickname of the TRILL header is RB5 itself, indicating that the TRILL data frame has reached the destination end of the TRILL network. Decapsulation is performed, and the outer Ethernet header and TRILL header are stripped off, leaving only the raw Ethernet frame. Ordinary L2 unicast forwarding is carried out according to the NativeDA and Native VLAN of the raw Ethernet frame, and the raw Ethernet frame finally reaches HostB.

- TRILL Multicast Data Frame Forwarding

TRILL supports multiple multicast distribution trees, and each multicast distribution tree is identified by the nickname of its root RB which is used as EgressNickname of this multicast distribution tree. In the TRILL network schematic below, one multicast distribution tree with RB3 as Root is shown. The red link represents the forwarding link participating in this distribution tree, while the dotted link will not participate in distribution tree forwarding. The forwarding link of each multicast distribution tree is calculated by the TRILL protocol.

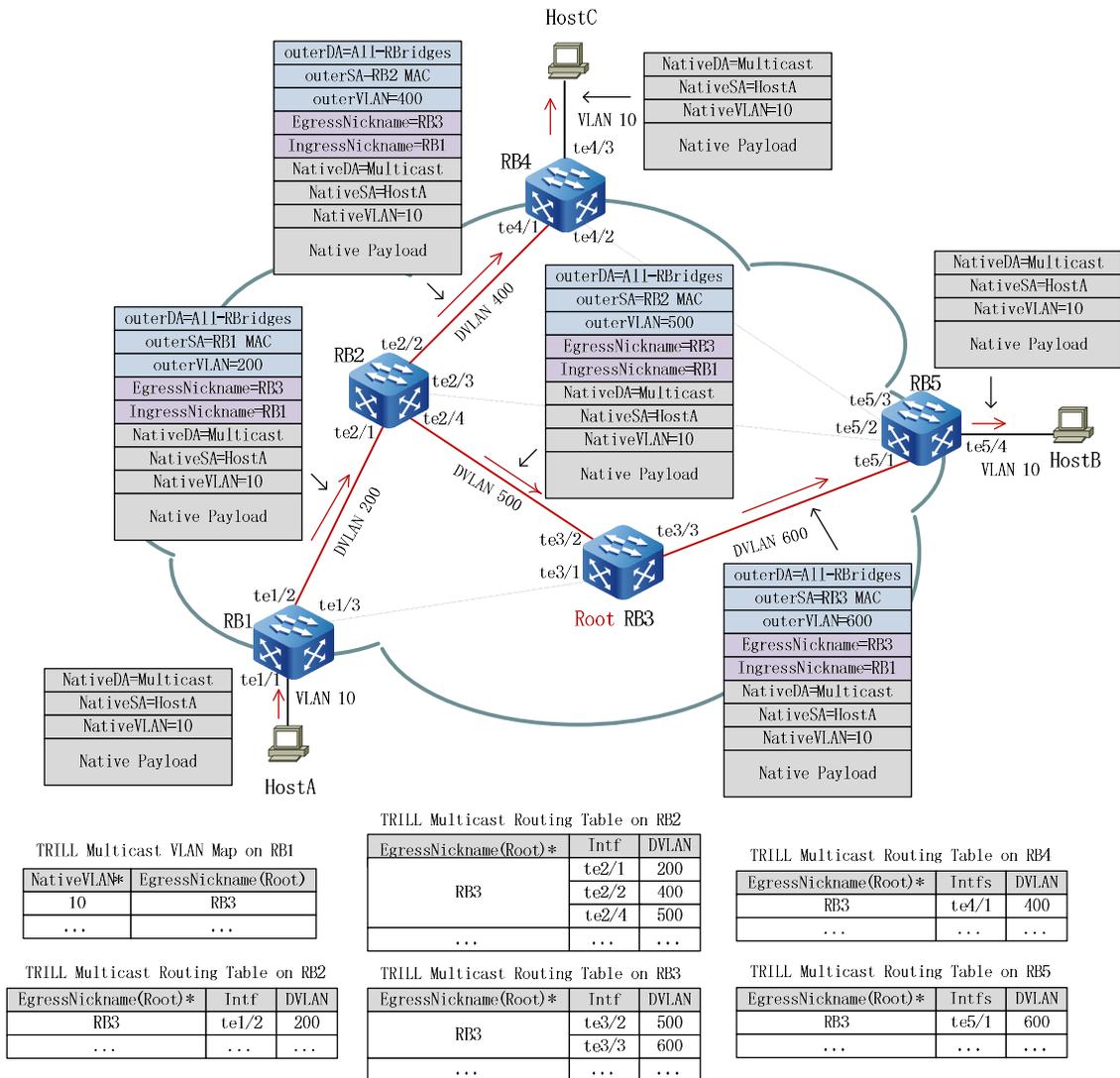


Figure 125-4 Example of TRILL Multicast Frame Forwarding Process

Each RB in the TRILL network stores the multicast routing table of each distribution tree. The multicast routing table of each distribution tree may contain one or more sub-entries. Each sub-entry is "Intf+DVLAN", indicating the egress port for forwarding TRILL multicast frames and the corresponding DVLAN. In addition, each edge RB in the TRILL network also stores the NativeVLAN to Root mapping relationship, namely, when there are multiple distribution trees in the network, which distribution tree should the multicast traffic of this VLAN should go through.

In this example, when RB1 receives a multicast packet from HostA, it first checks the NativeVLAN to Root mapping relationship, determines that the multicast packet of VLAN 10 should be forwarded via the multicast distribution tree with RB3 as Root, then uses RB3 as Root to check the TRILL multicast routing table, and learns that this distribution tree has only one sub-entry, namely, Intf te1/2+DVLAN 200. Then the raw multicast packet is encapsulated with outer Ethernet header and TRILL header. The outer VLAN of the outer Ethernet header is 200, outerDA is the fixed value All-RBridges, outerSA is RB1's own MAC,

and IngressNickname of the TRILL header is RB1's own nickname, EgressNickname is the nickname of the root RB3, and M flag is set to 1, indicating that this TRILL frame is a multicast frame. After the TRILL frame is encapsulated, it is forwarded from te1/2 of RB1.

When RB2 receives the TRILL multicast frame forwarded by RB1, it uses EgressNickname (RB3) of the TRILL header as Root to check the TRILL multicast routing table and learns that this distribution tree has three sub-entries, namely, Intf te2/1 +DVLAN 200, Intf te2/2+DVLAN 400, Intf te2/4+DVLAN 500, among them the sub-entry Intf te2/1+DVLAN 200 corresponds to the port and DVLAN where the multicast packet comes in, so RB2 should forward this multicast frame according to the other two sub-entries. RB2 reduces the hop count of the TRILL header by 1, and then forwards it from te2/2 and te2/4 after changing the encapsulation of the outer Ethernet header.

When RB3 receives the TRILL multicast frame forwarded by RB2, it uses EgressNickname (RB3) of the TRILL header as Root to check the TRILL multicast routing table and learns that this distribution tree has two sub-entries, namely, Intf te3/ 2+DVLAN 500 and Intf te3/3+DVLAN 600, in which the sub-entry Intf te3/2+DVLAN 500 corresponds to the port and DVLAN where the multicast packet comes in, so RB3 should forward the multicast frame according to the other sub-entry. RB3 reduces the hop count in the TRILL header by 1, and then forwards it from te3/3 after changing the encapsulation of the outer Ethernet header.

When RB4 receives the TRILL multicast frame forwarded by RB2, it uses EgressNickname (RB3) of the TRILL header as Root to check the TRILL multicast routing table and learns that this distribution tree has only one sub-entry, namely, Intf te4/ 1+DVLAN 400, which corresponds to the port and DVLAN where the multicast packet comes in, so RB4 does not continue to forward the multicast frame in the TRILL network. However, because RB4 is an edge RB, the multicast frame is decapsulated, the outer Ethernet header and TRILL header are stripped off, leaving only the raw Ethernet frame. Ordinary L2 multicast forwarding is carried out according to the NativeDA and Native VLAN of the raw Ethernet frame, and HostB receives the raw Ethernet frame.

When RB5 receives the TRILL multicast frame forwarded by RB3, it uses EgressNickname (RB3) of the TRILL header as Root to check the TRILL multicast routing table and learns that this distribution tree has only one sub-entry, namely, Intf te5/ 1+DVLAN 600, which corresponds to the port and DVLAN where the multicast packet comes in, so RB5 does not continue to forward the multicast frame in the TRILL network. However, because RB4 is an edge RB, the multicast frame is decapsulated, the outer Ethernet header and TRILL header are stripped off, leaving only the raw Ethernet frame. Ordinary L2 multicast forwarding is carried out according to the NativeDA and Native VLAN of the raw Ethernet frame, and HostC receives the raw Ethernet frame.

## 125.2 TRILL Function Configuration

Table 125-1 Port Security Basic Function Configuration List

Configuration Task	
Enable the TRILL protocol globally	Enable the TRILL protocol globally
Configure system id and nickname	Configure RB's system id
	Configure RB's nickname
Enable the TRILL protocol on the port	Configure the type of TRILL port
	Enable the TRILL protocol on the port
Configure the DRB priority of the port	Configure the DRB priority of the port
Configure advertising VLAN and designated VLAN of the port	Configure advertising VLAN of the port
	Configure designated VLAN of the port
Configure VLAN Forwarder	Configure VLAN Forwarder
Configure pseudo-node mode of the port	Configure pseudo-node mode of the port
Configure link overhead of the port	Configure link overhead of the port
Configure campus wide MTU	Configure campus wide MTU
Configure Hello packet sending interval	Configure Hello packet sending interval
Configure CSNP packet sending interval	Configure CSNP packet sending interval
Configure LSP related time parameters	Configure the maximum lifetime and refresh interval of LSP packets
	Configure LSP retransmission interval of the port
	Configure LSP regeneration interval
	Configure the minimum interval for sending LSP on the port

Configuration Task	
Configure to ignore LSP checksum errors	Configure to ignore LSP checksum errors
Configure SPF algorithm interval	Configure SPF algorithm interval
Configure the number of distribution trees	Configure the maximum number of distribution trees that native RB can support
	Configure the number of distribution trees that native RB desires to compute in the entire network
Configure TRILL gateway	Configure the TRILL gateway function to forwarding TRILL services via L3 interface

### 125.2.1 Enable the TRILL Protocol Globally

When configuring the TRILL protocol, you must first enable the TRILL protocol globally before configuring other TRILL features.

#### Configuration Condition

None

#### Enable the TRILL Protocol Globally

Enable the TRILL protocol globally and enter the TRILL view.

Table 125-2 Enabling the TRILL Protocol Globally

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enable the TRILL protocol globally and enter the TRILL view	<b>trill</b>	Mandatory By default, the TRILL protocol is not enabled globally

## 125.2.2 Configure System ID and Nickname

System id and nickname are important identifiers of RB in the TRILL network. They can be automatically assigned by the system or manually configured.

### Configuration Condition

None

### Configure RB's system ID

System id is system identifier of RB in the TRILL network.

Table 125-3 Configuring RB's system id

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter TRILL view	<b>trill</b>	-
Configure RB's system id	<b>system-id</b> <i>system-id</i>	Optional By default, RB will automatically generate one system id based on its MAC address

---

### Note

- System ids of RBs in the TRILL network must be different from each other.
- 

### Configure RB's Nickname

Nickname is address identifier of RB in the TRILL network.

Each nickname has a priority. When nickname conflict occurs between different RBs in the TRILL network, the one with the lower priority will automatically abandon the original nickname and reselect a new nickname.

Each nickname has a root priority. The higher the root priority, the more likely the nickname will become the root to a multicast tree.

Table 125-4 Configuring RB's nickname

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter TRILL view	<b>trill</b>	-
Configure RB's nickname	<b>nickname</b> <i>nickname</i>	Optional By default, RB will automatically generate one nickname
Configure the priority of nickname	<b>nickname</b> <i>nickname</i> <b>priority</b> <i>priority</i>	Optional By default, the priority of nickname is manually configured as 192
Configure the root priority of nickname	<b>nickname</b> <i>nickname</i> <b>root-priority</b> <i>root-priority</i>	By default, the root priority of nickname is manually configured as 32768

---

## Note

- Only the manually configured priority and root priority of the nickname can be modified. The automatically generated priority of nickname is fixedly 64 and must not be modified; the automatically generated root priority of nickname is fixedly 32768 and must not be modified.
- Up to 3 nicknames can be manually configured for One RB, among them the nickname with the highest priority will become sender nickname (used as ingress nickname for encapsulating the TRILL packet).
- The number of multicast distribution trees is determined by RB having the nickname with

---

the highest root priority throughout the network, but must not exceed the minimum number of distribution trees that each RB can support.

---

### 125.2.3 Enable the TRILL Protocol on the Port

To enable the TRILL protocol on the port, it is recommended to configure the type of TRILL port first, and then enable the TRILL protocol on the port.

#### Configuration Condition

You must enable the TRILL protocol globally before enabling the TRILL protocol on the port.

#### Configure the Type of TRILL Port

There are four types of TRILL port: Access, Trunk, P2P, and Hybrid.

Table 125-5 Configuring the Type of TRILL Port

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Configure the type of TRILL port	<b>trill link-type { access   trunk   p2p   hybrid}</b>	Mandatory  <b>access:</b> Configure the type of this TRILL port as Access

Step	Command	Description
		<p><b>trunk:</b> Configure the type of this TRILL port as Trunk</p> <p><b>p2p:</b> Configure the type of this TRILL port as P2P</p> <p>hybrid: Configure the type of this TRILL port as Hybrid</p> <p>By default, the type of the TRILL port is Access.</p>

## Note

- When the VLAN mode of the port is Access, the TRILL type of the port can only be Access, not Trunk or P2P. When the VLAN mode of the port is Trunk or Hybrid, the TRILL type of this port is not limited, and it can be any one of Access/Trunk/P2P/Hybrid.
- For the port that is added into any interface vlan, its TRILL type cannot be set to Trunk, P2P or Hybrid. During networking and configuration, please avoid enabling the TRILL protocol on ports that are added into any interface VLAN.
- Make sure the neighbor ports on the same link are of the same type, otherwise the neighbor relationship cannot be established.
- During networking and configuration, for Trunk, P2P, or Hybrid ports, please avoid establishing more than one TRILL neighbor on the same port of RB. Access ports are not limited so.

## Enable the TRILL Protocol on the Port

Table 125-6 Enabling the TRILL Protocol on the Port

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.

Step	Command	Description
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enable the TRILL protocol on the port	<b>trill enable</b>	Mandatory  By default, the TRILL protocol is not enabled on the port

---

## Note

- During networking and configuration, please avoid both TRILL-enabled port and TRILL-enabled port present among the member ports of the same VLAN. In other words, if certain VLAN on the switch is used for TRILL, please do not use this VLAN for other purposes.
  - The enabling of the TRILL protocol on the port is mutually exclusive with the enabling of functions such as spanning tree, EIPS, and ULPP. To enable the TRILL protocol on a port, you must first disable the spanning tree, EIPS, and ULPP functions of this port, and then enable the TRILL protocol.
- 

### 125.2.4 Configure the DRB Priority of the Port

DRB resolution is required when the link type is broadcast link. The resolution rules are as follows: RB with the highest DRB priority is chosen as DRB first; if two RBs have the same DRB priority, the one with the largest MAC address will be chosen as DRB.

#### Configuration Condition

None

### Configure the DRB Priority of the Port

Table 125-7 Configuring the DRB Priority of the Port

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected. After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Configure the DRB priority of the TRILL port	<b>trill drb-priority</b> <i>priority</i>	Optional priority: The value range is 0-127, the larger the value, the higher the priority By default, the DRB priority of the port is 64

---

### Note

- The DRB priority takes effect only when the link type is broadcast link. Because there is no need for DRB resolution, when the link type is point-to-point link, the DRB priority has no effect although it can be configured.
-

## 125.2.5 Configure Advertising VLAN and Designated VLAN of the Port

Neighboring RBs exchange Hello packets to discover neighbors and establish neighbor relationships. Hello packets are sent in the following VLAN sets according to different situations:

- The port being of Access type and a DRB:
  - Enable VLAN  $n$  (designated VLAN  $\cup$  advertising VLAN)
- The port being of Access type but not a DRB:
  - Enable VLAN  $n$  (designated VLAN  $\cup$  (advertising VLAN  $\cap$  AVF VLAN))
- The port being of Trunk type, P2P type or Hybrid type:
  - Enable VLAN  $n$  designated VLAN

The above "enable VLAN" refers to the set of VLANs that have been created and allowed to pass through the port. " $\cap$ " and " $\cup$ " are set operators, which represent "intersection" and "union" respectively.

All TRILL protocol packets and all TRILL data packets except Hello packets are sent via the designated VLAN.

### Configuration Condition

None

### Configure Advertising VLAN of the Port

Configure the advertising VLAN of the TRILL port to limit the VLAN range for the port to send Hello packets.

Table 125-8 Configuring Advertising VLAN of the Port

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration

Step	Command	Description
		takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Configure advertising VLAN of the TRILL port	<b>trill announcing-vlan</b> { <i>vlan-list</i>   <b>null</b>   <b>default</b> }	<p>Optional</p> <p><b>vlan-list</b>: to represent the set of configured advertising VLANs</p> <p><b>null</b>: indicating that there are no advertising VLANs, with the port only sending Hello packets in the designated VLAN</p> <p><b>default</b>: Restore the advertising VLAN to the default</p> <p>By default, no advertising VLAN is configured. At this point, the advertising VLAN is in the same range as the enable VLAN.</p>

---

## Note

- To prevent the device from consuming too much CPU resources due to sending numerous Hello packets, please try to narrow the range of the advertising VLANs. In particular, in the conventional networking environment, if each RB on the link is one device from our company, it is recommended to configure the advertising VLAN to null.
- 

### Configure Designated VLAN of the Port

Table 125-9 Configuring Designated VLAN of the Port

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Configure designated VLAN of the TRILL port	<b>trill desired-designated-vlan</b> { <i>vlan-id</i>   <b>default</b> }	Optional  vlan-id: Represent the desired designated VLAN  <b>default</b> : Restore the designated VLAN to the default  By default, no designated VLAN is configured. In this case, the designated VLAN is the minimum enable VLAN of the port

 **Note**

- Make sure that the configured designated VLAN is within the range of the port enabled

---

VLAN, otherwise neighbor relationship may not be established.

- It is recommended to configure the designated VLANs of adjacent ports to the same value. In this way, the designated VLANs remain unchanged upon DRB changes, thereby avoiding link flapping.
- 

## 125.2.6 Configure VLAN Forwarder

By default, DRB assumes AVFs of all VLANs. However, you can also designate certain neighbor RB to assume AVFs of some VLANs through manual configuration.

### Configuration Condition

None

### Configure VLAN Forwarder

Table 125-10 Configuring VLAN Forwarder

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Configure certain neighbor RB as the AVF for some VLANs	<b>trill vlan-forwarder</b> <b>nickname</b> <i>nickname</i> <b>vlan</b> <i>vlan-list</i>	Optional

---

## Note

- The configuration of VLAN Forwarder only takes effect when the port is the DRB of the link where it is located. Although the VLAN Forwarder may be configured when the port is not the DRB of the link where it is located, the configuration will not take effect.
  - If the neighbor RB has multiple nicknames, the nickname configured here must be sender nickname of this RB.
  - For the remaining VLANs that are not subjected to VLAN Forwarder configuration: (1) if the VLAN is enabled by the DRB, the DRB assumes the AVF for this VLAN; (2) if the VLAN is not enabled by the DRB, certain neighbor RB with this VLAN enabled is randomly selected by the DRB to assume the AVF for this VLAN.
- 

### 125.2.7 Configure Pseudo-node Mode of the Port

When there are more than two RBs on broadcast link (that is, three or more RBs are connected over common L2 switching network), you should enable the pseudo-node mode. After the pseudo-node mode is enabled, the DRB from resolution is responsible for creating pseudo-nodes and generating pseudo-node LSPs for describing which RBs are on this broadcast network.

#### Configuration Condition

None

#### Configure Pseudo-node Mode of the Port

Table 125-11 Configuring Pseudo-node Mode of the Port

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected. After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	

Step	Command	Description
		current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enable the pseudo-node mode on the port	<b>trill pseudo-node</b>	Optional By default, the pseudo-node mode of the port is disabled

---

### Note

- It is recommended to enable the pseudo-node mode for all TRILL ports on broadcast link when there are more than two RBs present on this broadcast link.
  - You have no need to enable the pseudo-node mode when there is only one or two RBs on broadcast link.
  - Since the pseudo-node mode does not work on point-to-point link, you have no need to enable the pseudo-node mode on the point-to-point link.
- 

## 125.2.8 Configure Link Overhead of the Port

By default, link overhead of TRILL port is automatically calculated by the system based on link bandwidth. However, the user can also modify it through manual configuration.

Auto calculation formula: link overhead value = 20000000 / speed (where speed is port rate in Mbps)

### Configuration Condition

None

### Configure Link Overhead of the Port

Table 125-12 Configuring Pseudo-node Mode of the Port

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Configure link overhead of the port	<b>trill wide-metric</b> { <i>value</i>   <b>default</b> }	Optional  <i>value</i> : Link overhead value configured by user. The greater the value, the higher routing overhead, and the more difficult the link is to be selected  <b>default</b> : Restore the link overhead value to auto calculation  By default, the link overhead value of the port is automatically calculated by the system

---

 **Note**

- 
- The link overhead value of TRILL port refers to outbound overhead value, that is, value of overhead from native RB to the opposite RB through the link.
- 

## 125.2.9 Configure Campus-wide MTU

In TRILL network, each RB advertises out its own campus wide MTU, and receives campus wide MTUs sent by other RBs, thereby selecting the smallest campus wide MTU in the entire network. The length of LSP cannot exceed the smallest campus wide MTU of the entire network when LSP packaging is performed on RB. This ensures that the LSP sent by itself can be transmitted on any link in the TRILL network without being discarded.

### Configuration Condition

None

### Configure Campus-wide MTU

Table 125-13 Configuring campus wide MTU

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Port campus wide MTU	<b>trill campus-wide-mtu</b> <i>size</i>	Optional By default, campus wide MTU is 1470 bytes

---

### Note

- The length of campus wide MTU includes 18 bytes of Ethernet header and the length of LSPDU. For example, the smallest campus wide MTU of the entire network is 1470 bytes when all RBs in the entire network adopt the default campus wide MTU. In this case, maximum of PDU Length is  $1470 - 18 = 1452$  bytes upon LSP packaging for each RB.
  - The MTU value of the port should be greater than campus wide MTU, otherwise TRILL LSP will not be sent normally.
-

## 125.2.10 Configure Hello Packet Sending Interval

Each TRILL port of RB must periodically send Hello packets to establish and maintain neighbor relationship. The product of Hello packet sending interval and the keepalive multiplier is neighbor relationship keepalive time. RB informs its neighbor of the keepalive time via Hello packet. It is considered that the neighbor relationship has been DOWN if this neighbor does not receive the Hello packet within the keepalive time.

### Configuration Condition

None

### Configure Hello Packet Sending Interval

Table 125-14 Configuring Hello Packet Sending Interval

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected. After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Configure Hello packet sending interval	<b>trill hello-interval</b> <i>interval</i>	Optional By default, the Hello packet sending interval is 10 seconds

Step	Command	Description
Configure keepalive multiplier of neighbor relationship	<b>trill holding-multiplier</b> <i>number</i>	Optional By default, the keepalive multiplier of neighbor relationship is 3

## Note

- On a broadcast link, the interval at which DRB sends Hello packets is 1/3 of sending interval parameter to ensure that DRB failure can be quickly detected. For example, by default, the interval at which non-DRB sends Hello packets is 10 seconds, while the interval at which DRB sends Hello packets is 3.3 seconds.

### 125.2.11 Configure CSNP Packet Sending Interval

On a broadcast link, DRB must periodically send CSNP packets to synchronize LSPDBs throughout the network.

#### Configuration Condition

None

#### Configure CSNP Packet Sending Interval

Table 125-15 Configuring CSNP Packet Sending Interval

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected. After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	

Step	Command	Description
		takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Configure CSNP packet sending interval	<b>trill csnp-interval</b> <i>interval</i>	Optional By default, the CSNP packet sending interval is 10 seconds

## 125.2.12 Configure LSP Related Time Parameters

You may adjust the following LSP related time parameters via this configuration:

- **Maximum lifetime of LSP:** The maximum lifetime of an LSP is the maximum survival time of the LSP on the device. If the device has not received update of the LSP, the LSP will be deleted when the maximum lifetime is up.
- **LSP refresh interval:** For one locally generated LSP, the LSP must be refreshed periodically even if there is no change in the content of the LSP. In this way, other devices in the network may be avoided aging the LSP, thereby keeping the LSP alive.
- **Interval for port retransmission of LSP:** On a P2P link, if the port does not receive PSNP response from the peer end within a period of time after the port sends an LSP packet, it needs to resend the LSP packet.
- **LSP regeneration interval:** the device needs to regenerate the LSP to advertise these changes in case of a network topology change. The device provides a limit for the case that each time an LSP is regenerated, there must be an interval since the last LSP is generated, so as to suppress the excessive occupation of bandwidth resources and CPU resources that may be caused by frequent changes in the network topology.
- **Minimum interval for the port to send LSPs:** When the port needs to send a large number of LSPs, the LSPs are not all sent at once, but sent in multiple splits. There is an interval for two sending operations, which makes the sending process relatively smooth and prevents a lot of bandwidth resources and CPU resources from being consumed instantly.

### Configuration Condition

None

### Configure the Maximum lifetime and Refresh Interval of the LSP

Table 125-16 Configuring the Maximum lifetime and Refresh Interval of the LSP

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter TRILL view	<b>trill</b>	-
Configure the maximum lifetime of LSP	<b>max-lsp-lifetime</b> <i>time</i>	Optional By default, the maximum lifetime of an LSP is 1200 seconds
Configure refresh interval of LSP	<b>lsp-refresh-interval</b> <i>interval</i>	Optional By default, the refresh interval of LSP is 900 seconds

---

#### Note

- When configuring, note that the maximum lifetime of an LSP should be greater than the refresh interval, and it is recommended that the difference between them be at least 300 seconds. In this way, the new LSP can reach all RBs in the network before the old LSP is aged.
- 

### Configure LSP Retransmission Interval of the Port

Table 125-17 Configuring LSP Retransmission Interval of the Port

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected.  After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Configure LSP retransmission interval of the port	<b>trill lsp-retransmit-interval</b> <i>interval</i>	Optional  By default, the LSP retransmission interval of the port is 5 seconds

## Note

- Only the P2P link will retransmit the LSP, and the broadcast link will not retransmit the LSP, so this configuration does not take effect on the broadcast link.

## Configure LSP Regeneration Interval

Table 125-18 Configuring LSP Regeneration Interval

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Enter TRILL view	<b>trill</b>	-
Configure LSP regeneration interval	<b>lsp-gen-interval</b> <i>interval</i>	Optional By default, the LSP regeneration interval is 30 milliseconds

### Configure the Minimum Interval for Sending LSP on the Port

Table 125-19 Configuring the Minimum Interval for Sending LSP on the Port

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the layer-2 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	At least one option must be selected. After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter Aggregation Group Configuration Mode	<b>interface link-aggregation</b> <i>link-aggregation-id</i>	
Configure the minimum interval for sending LSP on the port	<b>trill lsp-tx-interval</b> <i>interval</i>	Optional By default, the port sends LSP at an minimum interval of 33 milliseconds

## 125.2.13 Configure to Ignore LSP Checksum Errors

When the RB receives an LSP packet, it needs to perform checksum calculation on the received LSP, and compare the calculated checksum with that carried in the LSP packet. By default, if the checksum in the packet is found to be inconsistent with the calculated checksum, the LSP will be discarded without processing; you can also configure to ignore checksum errors, the packet will be processed as a normal packet even if the checksum errors of the LSP are found.

### Configuration Condition

None

### Configure to Ignore LSP Checksum Errors

Table 125-20 Configuring to Ignore LSP Checksum Errors

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter TRILL view	<b>trill</b>	-
Configure to ignore LSP checksum errors	<b>ignore-lsp-errors</b>	Optional By default, LSP checksum errors are not ignored

## 125.2.14 Configure SPF Algorithm Interval

When the network status changes, the TRILL protocol uses the SPF algorithm for route computing. However, when the network status is unstable, frequent SPF calculations will consume a large amount of CPU resources of the system, affecting the operation of normal services. Therefore, there must be a certain interval between two consecutive SPF calculations. The system reduces the SPF calculation interval to the minimum-interval when the network changes infrequently, and performs corresponding penalties, i.e., appropriately extends the SPF calculation interval when the network changes frequently, without exceeding the maximum-interval at most.

### Configuration Condition

None

### Configure SPF Algorithm Interval

Table 125-21 Configuring to Ignore LSP Checksum Errors

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter TRILL view	<b>trill</b>	-
Configure SPF algorithm interval	<b>spf-interval</b> <i>max-interval</i> <i>min-interval</i>	Optional  By default, the maximum interval of the SPF algorithm is 50 seconds and the minimum interval is 500 seconds.

### 125.2.15 Configure the Number of Distribution Trees

In TRILL network, each RB encapsulates in the LSP for transmission, the maximum number of distribution trees that this RB can support and the number of distribution trees that the RB desires to compute in the entire network.

Based on the minimums of the number of distribution trees that the RB with the highest distribution tree root priority desires for calculation in the entire network and the maximum number of distribution trees that the various RBs in the network can support, each RB uses the smaller one (assumed as n) of the two values as the number of distribution trees to be computed by this RB. The nicknames of all RBs in the entire network are then sorted from highest priority to lowest, and the first n nicknames are used as the distribution tree root bridge list used by this RB for calculation.

#### Configuration Condition

None

#### Configure the Maximum Number of Distribution Trees that Native RB Can Support

Table 125-22 Configuring the Maximum Number of Distribution Trees that Native RB can Support

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-

Step	Command	Description
Enter TRILL view	<b>trill</b>	-
Configure the maximum number of distribution trees that native RB can support	<b>dtrees maximum <i>num</i></b>	Optional By default, the maximum number of distribution trees that native RB can support is 8

### Configure the Number of Distribution Trees that Native RB Desires to Compute in the Entire Network

Table 125-23 Configuring the Number of Distribution Trees That Native RB Desires to Compute in the Entire Network

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter TRILL view	<b>trill</b>	-
Configure the number of distribution trees that native RB desires to compute in the entire network	<b>dtrees number-to-compute <i>num</i></b>	Optional By default, the RB desires to compute 1 distribution tree in the entire network

#### Note

- Only when native RB is the RB having the nickname with the highest root priority in the entire network, the number of distribution trees that the native RB desires to compute in the entire network will take effect.

## 125.2.16 TRILL Monitoring and Maintaining

Table 125-24 TRILL Monitoring and Maintaining

Command	Description
<b>show trill brief</b>	Show global brief of TRILL
<b>show trill interface brief</b>	Show TRILL brief of all ports
<b>show trill { interface <i>interface-name</i>   interface link-aggregation <i>link-aggregation-id</i> }</b>	Show TRILL running information of the port
<b>show trill neighbor brief</b>	Show the brief of all TRILL neighbors
<b>show trill neighbor [ interface <i>interface-name</i>   interface link-aggregation <i>link-aggregation-id</i> ]</b>	Show TRILL neighbor information on the port
<b>show trill vlan-forwarder [ interface <i>interface-name</i>   interface link-aggregation <i>link-aggregation-id</i> ]</b>	Show AVF information on the port
<b>show trill nickname-database</b>	Show the nickname database for the entire network
<b>show trill lspdb [ detail ]</b>	Show all LSP information in the LSPDB
<b>show trill topology</b>	Show the topology information of the TRILL unicast path
<b>show trill dtrees [ <i>nickname</i> ]</b>	Show TRILL distribution tree information
<b>show trill unicast-route</b>	Show TRILL unicast routing table entries

Command	Description
<b>show trill multicast-route [ tree-root nickname ]</b>	Show TRILL multicast routing table entries
<b>show trill rpf-table [ nickname ]</b>	Show TRILL RPF entries
<b>show trill counters rbridge</b>	Show global TRILL statistics of the RB
<b>show trill counters interface all</b>	Show TRILL statistics of all ports
<b>show trill counters { interface interface-name   interface link-aggregation link-aggregation-id }</b>	Show TRILL statistics of the designated port
<b>clear trill counters rbridge</b>	Clear the global TRILL statistics of the RB
<b>clear trill counters interface all</b>	Clear the TRILL statistics of all ports
<b>clear trill counters { interface interface-name   interface link-aggregation link-aggregation-id }</b>	Clear the TRILL statistics of the designated port
Command	Description
<b>show trill gateway</b>	Show all TRILL gateways in the TRILL network
<b>show trill gateway interface</b>	Show all TRILL gateways created by native RB

## 125.3 TRILL Gateway Function Configuration

Table 125-25 Basic Function Configuration List for TRILL Gateway

Configuration Task	
Enable the TRILL gateway globally	Enable the TRILL gateway globally

### 125.3.1 Configure TRILL Gateway

The TRILL gateway allows the RB to support the L3 route forwarding function.

The TRILL gateway is directly deployed on the RB device running the TRILL protocol. When configuring the TRILL gateway, you must first create an Interface VLAN interface and enable the TRILL gateway function on this interface. The gateway RB will be synchronized to the entire TRILL network through the LSP, and each access RB computes a path to the TRILL gateway according to its unicast route and installs to the static MAC address arriving at the gateway, thereby realizing the L3 route forwarding function for TRILL services.

#### Configuration Condition

You must enable the TRILL protocol globally before enabling the TRILL gateway on the interface.

#### Configure TRILL Gateway

Table 125-26 Configuring TRILL Gateway

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter the interface view	<b>interface vlan <i>vlan-id</i></b>	You must create a L3 interface before enabling the TRILL gateway,
Configure TRILL gateway	<b>trill gateway enable</b>	Mandatory  By default, the TRILL gateway is not enabled.

#### Note

- In the TRILL gateway application scenario, to complete the L3 route forwarding function

---

of the TRILL gateway, you must configure all TRILL ports of the TRILL gateway as Hybrid-type ports.

---

## 125.4 Typical Configuration Example of TRILL

### 125.4.1 Configure Basic Functions of TRILL

#### Network Requirements

- TRILL is enabled for RB1-RB5 globally.
- Te0/1-Te0/3 ports of RB1-RB2 and Te0/1-Te0/2 ports of RB3-RB5 are configured as Trunk type TRILL ports, so that RB1-RB5 can learn the TRILL route from each other.
- The Te0/4 ports of RB1-RB2 and the Te0/3 ports of RB3-RB5 are configured as ACCESS-type TRILL ports for connecting to a common L2 network or terminal device to allow for the access of the original data packets to the TRILL network.
- By Modifying the original TRILL port type of RB1-RB5 from Trunk to P2P, the convergence of the TRILL network is accelerated.

#### Network Topology

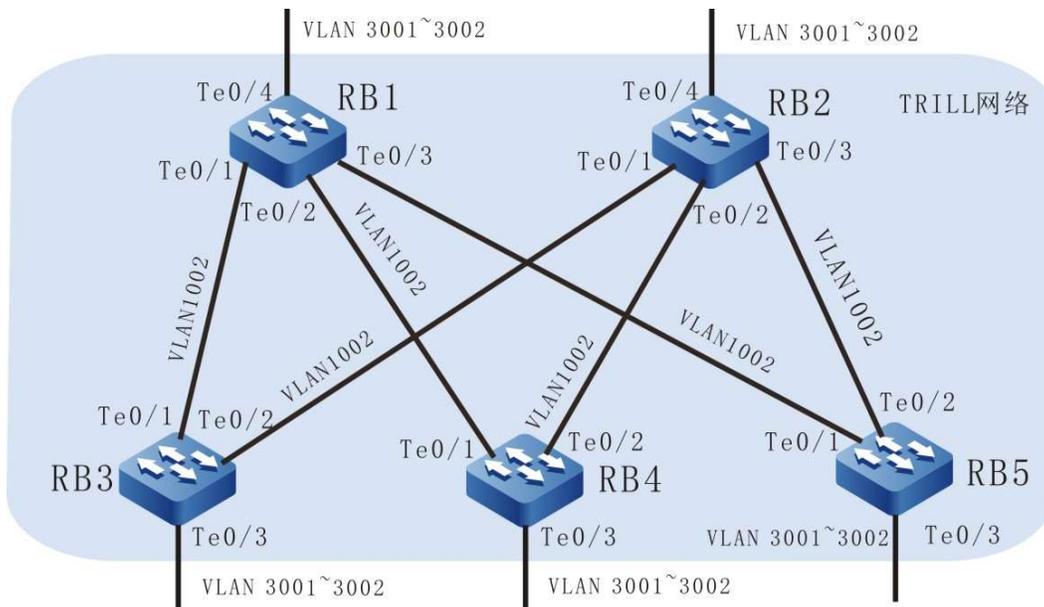


Figure 125-5 Configuring TRILL Network Topology

#### Configuration Steps

Step 1: Configure to add the ports RB1 to RB5 into the VLAN in Trunk mode. (Omitted)

Step 2: Configure to enable TRILL globally for RB1-RB5.

#Configure to enable TRILL globally on RB1 and configure Nickname as 0x0001.

```
RB1#configure terminal
RB1(config)#trill
RB1(config-trill)#nickname 0x0001
RB1(config-trill)#exit
```

#Configure to enable TRILL globally on RB2 and configure Nickname as 0x0002.

```
RB2#configure terminal
RB2(config)#trill
RB2(config-trill)#nickname 0x0002
RB2(config-trill)#exit
```

#Configure to enable TRILL globally on RB3 and configure Nickname as 0x0003.

```
RB3#configure terminal
RB3(config)#trill
RB3(config-trill)#nickname 0x0003
RB3(config-trill)#exit
```

#Configure to enable TRILL globally on RB4 and configure Nickname as 0x0004.

```
RB4#configure terminal
RB4(config)#trill
RB4(config-trill)#nickname 0x0004
RB4(config-trill)#exit
```

#Configure to enable TRILL globally on RB5 and configure Nickname as 0x0005.

```
RB5#configure terminal
RB5(config)#trill
RB5(config-trill)#nickname 0x0005
RB5(config-trill)#exit
```

Step 3: Configure the TRILL port type of RB1-RB5 as Trunk-type ports.

#Configure to shut down the spanning tree at the ports Te0/1~Te0/3 of RB1, and enable TRILL with the TRILL port type being Trunk, and the designated VLAN being 1002.

```
RB1(config)#interface tengigabitethernet 0/1
RB1(config-if-tengigabitethernet0/1)#no spanning-tree enable
RB1(config-if-tengigabitethernet0/1)#trill desired-designated-vlan 1002
RB1(config-if-tengigabitethernet0/1)#trill link-type trunk
RB1(config-if-tengigabitethernet0/1)#trill enable
RB1(config-if-tengigabitethernet0/1)#exit
RB1(config)#interface tengigabitethernet 0/2
RB1(config-if-tengigabitethernet0/2)#no spanning-tree enable
RB1(config-if-tengigabitethernet0/2)#trill desired-designated-vlan 1002
RB1(config-if-tengigabitethernet0/2)#trill link-type trunk
RB1(config-if-tengigabitethernet0/2)#trill enable
RB1(config-if-tengigabitethernet0/2)#exit
RB1(config)#interface tengigabitethernet 0/3
RB1(config-if-tengigabitethernet0/3)#no spanning-tree enable
RB1(config-if-tengigabitethernet0/3)#trill desired-designated-vlan 1002
```

```
RB1(config-if-tengigabitethernet0/3)#trill link-type trunk
RB1(config-if-tengigabitethernet0/3)#trill enable
RB1(config-if-tengigabitethernet0/3)#exit
```

#Configure to shut down the spanning tree at the ports Te0/1~Te0/3 of RB2, and enable TRILL with the TRILL port type being Trunk, and the designated VLAN being 1002.

```
RB2(config)#interface tengigabitethernet 0/1
RB2(config-if-tengigabitethernet0/1)#no spanning-tree enable
RB2(config-if-tengigabitethernet0/1)#trill desired-designated-vlan 1002
RB2(config-if-tengigabitethernet0/1)#trill link-type trunk
RB2(config-if-tengigabitethernet0/1)#trill enable
RB2(config-if-tengigabitethernet0/1)#exit
RB2(config)#interface tengigabitethernet 0/2
RB2(config-if-tengigabitethernet0/2)#no spanning-tree enable
RB2(config-if-tengigabitethernet0/2)#trill desired-designated-vlan 1002
RB2(config-if-tengigabitethernet0/2)#trill link-type trunk
RB2(config-if-tengigabitethernet0/2)#trill enable
RB2(config-if-tengigabitethernet0/2)#exit
RB2(config)#interface tengigabitethernet 0/3
RB2(config-if-tengigabitethernet0/3)#no spanning-tree enable
RB2(config-if-tengigabitethernet0/3)#trill desired-designated-vlan 1002
RB2(config-if-tengigabitethernet0/3)#trill link-type trunk
RB2(config-if-tengigabitethernet0/3)#trill enable
RB2(config-if-tengigabitethernet0/3)#exit
```

#Configure to shut down the spanning tree at the ports Te0/1~Te0/2 of RB3, and enable TRILL with the TRILL port type being Trunk, and the designated VLAN being 1002.

```
RB3(config)#interface tengigabitethernet 0/1
RB3(config-if-tengigabitethernet0/1)#no spanning-tree enable
RB3(config-if-tengigabitethernet0/1)#trill desired-designated-vlan 1002
RB3(config-if-tengigabitethernet0/1)#trill link-type trunk
RB3(config-if-tengigabitethernet0/1)#trill enable
RB3(config-if-tengigabitethernet0/1)#exit
RB3(config)#interface tengigabitethernet 0/2
RB3(config-if-tengigabitethernet0/2)#no spanning-tree enable
RB3(config-if-tengigabitethernet0/2)#trill desired-designated-vlan 1002
RB3(config-if-tengigabitethernet0/2)#trill link-type trunk
RB3(config-if-tengigabitethernet0/2)#trill enable
RB3(config-if-tengigabitethernet0/2)#exit
```

#Configure to shut down the spanning tree at the ports Te0/1~Te0/2 of RB4, and enable TRILL with the TRILL port type being Trunk, and the designated VLAN being 1002.

```
RB4(config)#interface tengigabitethernet 0/1
RB4(config-if-tengigabitethernet0/1)#no spanning-tree enable
RB4(config-if-tengigabitethernet0/1)#trill desired-designated-vlan 1002
RB4(config-if-tengigabitethernet0/1)#trill link-type trunk
RB4(config-if-tengigabitethernet0/1)#trill enable
RB4(config-if-tengigabitethernet0/1)#exit
RB4(config)#interface tengigabitethernet 0/2
RB4(config-if-tengigabitethernet0/2)#no spanning-tree enable
RB4(config-if-tengigabitethernet0/2)#trill desired-designated-vlan 1002
RB4(config-if-tengigabitethernet0/2)#trill link-type trunk
RB4(config-if-tengigabitethernet0/2)#trill enable
RB4(config-if-tengigabitethernet0/2)#exit
```

#Configure to shut down the spanning tree at the ports Te0/1~Te0/2 of RB5, and enable TRILL with the TRILL port type being Trunk, and the designated VLAN being 1002.

```

RB5(config)#interface tengigabitethernet 0/1
RB5(config-if-tengigabitethernet0/1)#no spanning-tree enable
RB5(config-if-tengigabitethernet0/1)#trill desired-designated-vlan 1002
RB5(config-if-tengigabitethernet0/1)#trill link-type trunk
RB5(config-if-tengigabitethernet0/1)#trill enable
RB5(config-if-tengigabitethernet0/1)#exit
RB5(config)#interface tengigabitethernet 0/2
RB5(config-if-tengigabitethernet0/2)#no spanning-tree enable
RB5(config-if-tengigabitethernet0/2)#trill desired-designated-vlan 1002
RB5(config-if-tengigabitethernet0/2)#trill link-type trunk
RB5(config-if-tengigabitethernet0/2)#trill enable
RB5(config-if-tengigabitethernet0/2)#exit

```

Step 4: Configure the TRILL port type of RB1-RB5 as Access type ports.

#Configure to shut down the spanning tree at the port Te0/4 of RB1, TRILL to advertise VLAN as NULL and TRILL port type as Access, and enable TRILL.

```

RB1(config)#interface tengigabitethernet 0/4
RB1(config-if-tengigabitethernet0/4)#no spanning-tree enable
RB1(config-if-tengigabitethernet0/4)#trill announcing-vlan null
RB1(config-if-tengigabitethernet0/4)#trill enable
RB1(config-if-tengigabitethernet0/4)#exit

```

#Configure to shut down the spanning tree at the port Te0/4 of RB2, TRILL to advertise VLAN as NULL and TRILL port type as Access, and enable TRILL.

```

RB2(config)#interface tengigabitethernet 0/4
RB2(config-if-tengigabitethernet0/4)#no spanning-tree enable
RB2(config-if-tengigabitethernet0/4)#trill announcing-vlan null
RB2(config-if-tengigabitethernet0/4)#trill enable
RB2(config-if-tengigabitethernet0/4)#exit

```

#Configure to shut down the spanning tree at the port Te0/3 of RB3, TRILL to advertise VLAN as NULL and TRILL port type as Access, and enable TRILL.

```

RB3(config)#interface tengigabitethernet 0/3
RB3(config-if-tengigabitethernet0/3)#no spanning-tree enable
RB3(config-if-tengigabitethernet0/3)#trill announcing-vlan null
RB3(config-if-tengigabitethernet0/3)#trill enable
RB3(config-if-tengigabitethernet0/3)#exit

```

#Configure to shut down the spanning tree at the port Te0/3 of RB4, TRILL to advertise VLAN as NULL and TRILL port type as Access, and enable TRILL.

```

RB4(config)#interface tengigabitethernet 0/3
RB4(config-if-tengigabitethernet0/3)#no spanning-tree enable
RB4(config-if-tengigabitethernet0/3)#trill announcing-vlan null
RB4(config-if-tengigabitethernet0/3)#trill enable
RB4(config-if-tengigabitethernet0/3)#exit

```

#Configure to shut down the spanning tree at the port Te0/3 of RB5, TRILL to advertise VLAN as NULL and TRILL port type as Access, and enable TRILL.

```

RB5(config)#interface tengigabitethernet 0/3
RB5(config-if-tengigabitethernet0/3)#no spanning-tree enable
RB5(config-if-tengigabitethernet0/3)#trill announcing-vlan null
RB5(config-if-tengigabitethernet0/3)#trill enable
RB5(config-if-tengigabitethernet0/3)#exit

```

#View all unicast route information of RB1.

```

RB1#show trill unicast-route
TRILL Unicast Forwarding Database
Eg_Nick  Eg_SysId  Metric HopCnt NH_Nick  NH_SysId  Interface      SNPA
0x0002   0001.7ace.820b 40000 002  0x0003  0001.7ace.820c  tengigabitethernet0/1  0001.7ace.820c
                                0x0004  0001.7ace.820d  tengigabitethernet0/2  0001.7ace.820d
                                0x0005  0001.7ace.820e  tengigabitethernet0/3  0001.7ace.820e
0x0003   0001.7ace.820c 20000 001  0x0003  0001.7ace.820c  tengigabitethernet0/1  0001.7ace.820c
0x0004   0001.7ace.820d 20000 001  0x0004  0001.7ace.820d  tengigabitethernet0/2  0001.7ace.820d
0x0005   0001.7ace.820e 20000 001  0x0005  0001.7ace.820e  tengigabitethernet0/3  0001.7ace.820e

```

On RB1, you can view the unicast route from RB1 to RB2-RB5.

#View the multicast route information of all distribution trees on RB1.

```

BR1#show trill multicast-route
Rbidge with highest priority tree root is 0x0005. LSP ID is 0001.7ace.820e.00-00

Dtree-number D-Tree_Name  D-tree-system-id Hop-count
01  0x0005  0001.7ace.820e  002  Dtree to use
Adj_Nickname  Adj_System_id  Interface      SNPA
0x0003  0001.7ace.820c  tengigabitethernet0/1  0001.7ace.820c
0x0004  0001.7ace.820d  tengigabitethernet0/2  0001.7ace.820d
0x0005  0001.7ace.820e  tengigabitethernet0/3  0001.7ace.820e

```

You can view the multicast route information of RB1 on RB1, with adjacencies including RB3-RB5.

#View information of all the distribution trees on RB1.

```

RB1#show trill dtrees
DTree Number: 1
Root nickname: 0x0005 System ID: 0001.7ace.820e
Distance to Root: 20000
Dtree state: USE , Nexthop Valid
Number of vlans: 2
List of vlans:
[3001-3002]

```

You can view the distribution tree information of RB1 on RB1, the root is 0x0005, and the AVF VLANs include 3001-3002.

#View all unicast route information of RB2.

```

RB2#show trill unicast-route
TRILL Unicast Forwarding Database
Eg_Nick  Eg_SysId  Metric HopCnt NH_Nick  NH_SysId  Interface      SNPA
0x0001   0001.7ace.820a 40000 002  0x0003  0001.7ace.820c  tengigabitethernet0/1  0001.7ace.820c
                                0x0004  0001.7ace.820d  tengigabitethernet0/2  0001.7ace.820d
                                0x0005  0001.7ace.820e  tengigabitethernet0/3  0001.7ace.820e
0x0003   0001.7ace.820c 20000 001  0x0003  0001.7ace.820c  tengigabitethernet0/1  0001.7ace.820c
0x0004   0001.7ace.820d 20000 001  0x0004  0001.7ace.820d  tengigabitethernet0/2  0001.7ace.820d
0x0005   0001.7ace.820e 20000 001  0x0005  0001.7ace.820e  tengigabitethernet0/3  0001.7ace.820e

```

On RB2, you can view the unicast route from RB2 to RB3-RB5.

#View the multicast route information of all distribution trees on RB2.

```

BR2#show trill multicast-route
Rbidge with highest priority tree root is 0x0005. LSP ID is 0001.7ace.820e.00-00

Dtree-number D-Tree_Name  D-tree-system-id Hop-count
01  0x0005  0001.7ace.820e  002  Dtree to use

```

Adj_Nickname	Adj_System_id	Interface	SNPA
0x0003	0001.7ace.820c	tengigabitethernet0/1	0001.7ace.820c
0x0004	0001.7ace.820d	tengigabitethernet0/2	0001.7ace.820d
0x0005	0001.7ace.820e	tengigabitethernet0/3	0001.7ace.820e

You can view the multicast route information of RB2 on RB2, with adjacencies including RB3-RB5.

#View information of all the distribution trees on RB2.

```
RB2#show trill dtrees
DTree Number: 1
Root nickname: 0x0005 System ID: 0001.7ace.820e
Distance to Root: 20000
Dtree state: USE , Nexthop Valid
Number of vlans: 2
List of vlans:
[3001-3002]
```

You can view the distribution tree information of RB2 on RB2, the root is 0x0005, and the AVF VLANs include 3001-3002.

#View all unicast route information of RB3.

```
RB3#show trill unicast-route
TRILL Unicast Forwarding Database
Eg_Nick Eg_SysId Metric HopCnt NH_Nick NH_SysId Interface SNPA
0x0001 0001.7ace.820a 20000 001 0x0001 0001.7ace.820a tengigabitethernet0/1 0001.7ace.820a
0x0002 0001.7ace.820b 20000 001 0x0002 0001.7ace.820b tengigabitethernet0/2 0001.7ace.820b
0x0004 0001.7ace.820d 40000 002 0x0001 0001.7ace.820a tengigabitethernet0/1 0001.7ace.820a
0x0002 0001.7ace.820b 40000 002 0x0002 0001.7ace.820b tengigabitethernet0/2 0001.7ace.820b
0x0005 0001.7ace.820e 40000 002 0x0001 0001.7ace.820a tengigabitethernet0/1 0001.7ace.820a
0x0002 0001.7ace.820b 40000 002 0x0002 0001.7ace.820b tengigabitethernet0/2 0001.7ace.820b
```

On RB3, you can view the unicast route from RB3 to RB1-RB2 and RB4-RB5.

#View the multicast route information of all distribution trees on RB3.

```
BR3#show trill multicast-route
Rbidge with highest priority tree root is 0x0005. LSP ID is 0001.7ace.820e.00-00

Dtree-number D-Tree_Name D-tree-system-id Hop-count
01 0x0005 0001.7ace.820e 002 Dtree to use
Adj_Nickname Adj_System_id Interface SNPA
0x0001 0001.7ace.820a tengigabitethernet0/1 0001.7ace.820a
0x0002 0001.7ace.820b tengigabitethernet0/2 0001.7ace.820b
```

You can view the multicast route information of RB3 on RB3, with adjacencies including RB1-RB2.

#View information of all the distribution trees on RB3.

```
RB3#show trill dtrees
DTree Number: 1
Root nickname: 0x0005 System ID: 0001.7ace.820e
Distance to Root: 40000
Dtree state: USE , Nexthop Valid
Number of vlans: 2
List of vlans:
[3001-3002]
```

You can view the distribution tree information of RB3 on RB3, the root is 0x0005, and the AVF VLANs include 3001-3002.

#The information viewed by RB4-RB5 is similar to that viewed by RB3. (Omitted)

Step 5: Configure the TRILL port type of RB1-RB5 as P2P type ports.

#Configure the TRILL port type of the ports Te0/1~Te0/3 of RB1 as P2P.

```
RB1(config)#interface tengigabitethernet 0/1
RB1(config-if-tengigabitethernet0/1)#trill link-type p2p
RB1(config-if-tengigabitethernet0/1)#exit
RB1(config)#interface tengigabitethernet 0/2
RB1(config-if-tengigabitethernet0/2)#trill link-type p2p
RB1(config-if-tengigabitethernet0/2)#exit
RB1(config)#interface tengigabitethernet 0/3
RB1(config-if-tengigabitethernet0/3)#trill link-type p2p
RB1(config-if-tengigabitethernet0/3)#exit
```

#Configure the TRILL port type of the ports Te0/1~Te0/3 of RB2 as P2P.

```
RB2(config)#interface tengigabitethernet 0/1
RB2(config-if-tengigabitethernet0/1)#trill link-type p2p
RB2(config-if-tengigabitethernet0/1)#exit
RB2(config)#interface tengigabitethernet 0/2
RB2(config-if-tengigabitethernet0/2)#trill link-type p2p
RB2(config-if-tengigabitethernet0/2)#exit
RB2(config)#interface tengigabitethernet 0/3
RB2(config-if-tengigabitethernet0/3)#trill link-type p2p
RB2(config-if-tengigabitethernet0/3)#exit
```

#Configure the TRILL port type of the ports Te0/1~Te0/2 of RB3 as P2P.

```
RB3(config)#interface tengigabitethernet 0/1
RB3(config-if-tengigabitethernet0/1)#trill link-type p2p
RB3(config-if-tengigabitethernet0/1)#exit
RB3(config)#interface tengigabitethernet 0/2
RB3(config-if-tengigabitethernet0/2)#trill link-type p2p
RB3(config-if-tengigabitethernet0/2)#exit
```

#Configure the TRILL port type of the ports Te0/1~Te0/2 of RB4 as P2P.

```
RB4(config)#interface tengigabitethernet 0/1
RB4(config-if-tengigabitethernet0/1)#trill link-type p2p
RB4(config-if-tengigabitethernet0/1)#exit
RB4(config)#interface tengigabitethernet 0/2
RB4(config-if-tengigabitethernet0/2)#trill link-type p2p
RB4(config-if-tengigabitethernet0/2)#exit
```

#Configure the TRILL port type of the ports Te0/1~Te0/2 of RB5 as P2P.

```
RB5(config)#interface tengigabitethernet 0/1
RB5(config-if-tengigabitethernet0/1)#trill link-type p2p
RB5(config-if-tengigabitethernet0/1)#exit
RB5(config)#interface tengigabitethernet 0/2
RB5(config-if-tengigabitethernet0/2)#trill link-type p2p
RB5(config-if-tengigabitethernet0/2)#exit
```

Step 6: Check the results.

#View all unicast route information of RB1.

```

RB1#show trill unicast-route
TRILL Unicast Forwarding Database
Eg_Nick Eg_SysId Metric HopCnt NH_Nick NH_SysId Interface SNPA
0x0002 0001.7ace.820b 40000 002 0x0003 0001.7ace.820c tengigabitethernet0/1 0001.7ace.820c
                                0x0004 0001.7ace.820d tengigabitethernet0/2 0001.7ace.820d
                                0x0005 0001.7ace.820e tengigabitethernet0/3 0001.7ace.820e
0x0003 0001.7ace.820c 20000 001 0x0003 0001.7ace.820c tengigabitethernet0/1 0001.7ace.820c
0x0004 0001.7ace.820d 20000 001 0x0004 0001.7ace.820d tengigabitethernet0/2 0001.7ace.820d
0x0005 0001.7ace.820e 20000 001 0x0005 0001.7ace.820e tengigabitethernet0/3 0001.7ace.820e

```

On RB1, you can view the unicast route from RB1 to RB2-RB5.

#View the multicast route information of all distribution trees on RB1.

```

BR1#show trill multicast-route
Rbidge with highest priority tree root is 0x0005. LSP ID is 0001.7ace.820e.00-00

Dtree-number D-Tree_Name D-tree-system-id Hop-count
01 0x0005 0001.7ace.820e 002 Dtree to use
Adj_Nickname Adj_System_id Interface SNPA
0x0003 0001.7ace.820c tengigabitethernet0/1 0001.7ace.820c
0x0004 0001.7ace.820d tengigabitethernet0/2 0001.7ace.820d
0x0005 0001.7ace.820e tengigabitethernet0/3 0001.7ace.820e

```

You can view the multicast route information of RB1 on RB1, with adjacencies including RB3-RB5.

#View information of all the distribution trees on RB1.

```

RB1#show trill dtrees
DTree Number: 1
Root nickname: 0x0005 System ID: 0001.7ace.820e
Distance to Root: 20000
Dtree state: USE , Nexthop Valid
Number of vlans: 2
List of vlans:
[3001-3002]

```

You can view the distribution tree information of RB1 on RB1, the root is 0x0005, and the AVF VLANs include 3001-3002.

#View all unicast route information of RB2.

```

RB2#show trill unicast-route
TRILL Unicast Forwarding Database
Eg_Nick Eg_SysId Metric HopCnt NH_Nick NH_SysId Interface SNPA
0x0001 0001.7ace.820a 40000 002 0x0003 0001.7ace.820c tengigabitethernet0/1 0001.7ace.820c
                                0x0004 0001.7ace.820d tengigabitethernet0/2 0001.7ace.820d
                                0x0005 0001.7ace.820e tengigabitethernet0/3 0001.7ace.820e
0x0003 0001.7ace.820c 20000 001 0x0003 0001.7ace.820c tengigabitethernet0/1 0001.7ace.820c
0x0004 0001.7ace.820d 20000 001 0x0004 0001.7ace.820d tengigabitethernet0/2 0001.7ace.820d
0x0005 0001.7ace.820e 20000 001 0x0005 0001.7ace.820e tengigabitethernet0/3 0001.7ace.820e

```

On RB2, you can view the unicast route from RB2 to RB3-RB5.

#View the multicast route information of all distribution trees on RB2.

```

BR2#show trill multicast-route
Rbidge with highest priority tree root is 0x0005. LSP ID is 0001.7ace.820e.00-00

Dtree-number D-Tree_Nam D-tree-system-id Hop-count
01 0x0005 0001.7ace.820e 002 Dtree to use
Adj_Nickname Adj_System_id Interface SNPA
0x0003 0001.7ace.820c tengigabitethernet0/1 0001.7ace.820c

```

```

0x0004    0001.7ace.820d    tengigabitethernet0/2    0001.7ace.820d
0x0005    0001.7ace.820e    tengigabitethernet0/3    0001.7ace.820e

```

You can view the multicast route information of RB2 on RB2, with adjacencies including RB3-RB5.

#View information of all the distribution trees on RB2.

```

RB2#show trill dtrees
DTree Number: 1
Root nickname: 0x0005 System ID: 0001.7ace.820e
Distance to Root: 20000
Dtree state: USE , Nexthop Valid
Number of vlans: 2
List of vlans:
[3001-3002]

```

You can view the distribution tree information of RB2 on RB2, the root is 0x0005, and the AVF VLANs include 3001-3002.

#View all unicast route information of RB3.

```

RB3#show trill unicast-route
TRILL Unicast Forwarding Database
Eg_Nick  Eg_SysId  Metric HopCnt NH_Nick  NH_SysId  Interface  SNPA
0x0001  0001.7ace.820a  20000  001  0x0001  0001.7ace.820a  tengigabitethernet0/1  0001.7ace.820a
0x0002  0001.7ace.820b  20000  001  0x0002  0001.7ace.820b  tengigabitethernet0/2  0001.7ace.820b
0x0004  0001.7ace.820d  40000  002  0x0001  0001.7ace.820a  tengigabitethernet0/1  0001.7ace.820a
                                0x0002  0001.7ace.820b  tengigabitethernet0/2  0001.7ace.820b
0x0005  0001.7ace.820e  40000  002  0x0001  0001.7ace.820a  tengigabitethernet0/1  0001.7ace.820a
                                0x0002  0001.7ace.820b  tengigabitethernet0/2  0001.7ace.820b

```

On RB3, you can view the unicast route from RB3 to RB1-RB2 and RB4-RB5.

#View the multicast route information of all distribution trees on RB3.

```

BR3#show trill multicast-route
Rbidge with highest priority tree root is 0x0005. LSP ID is 0001.7ace.820e.00-00

Dtree-number D-Tree_Name  D-tree-system-id Hop-count
01  0x0005  0001.7ace.820e  002  Dtree to use
Adj_Nickname  Adj_System_id  Interface  SNPA
0x0001  0001.7ace.820a  tengigabitethernet0/1  0001.7ace.820a
0x0002  0001.7ace.820b  tengigabitethernet0/2  0001.7ace.820b

```

You can view the multicast route information of RB3 on RB3, with adjacencies including RB1-RB2.

#View information of all the distribution trees on RB3.

```

RB3#show trill dtrees
DTree Number: 1
Root nickname: 0x0005 System ID: 0001.7ace.820e
Distance to Root: 40000
Dtree state: USE , Nexthop Valid
Number of vlans: 2
List of vlans:
[3001-3002]

```

You can view the distribution tree information of RB3 on RB3, the root is 0x0005, and the AVF VLANs include 3001-3002.

#The information viewed by RB4-RB5 is similar to that viewed by RB3. (Omitted)

## 125.4.2 Configure TRILL DRB Resolution

### Network Requirements

- TRILL is enabled for RB1-RB5 globally.
- Te0/1-Te0/3 ports of RB1-RB2 and Te0/1-Te0/2 ports of RB3-RB5 are configured as Trunk type TRILL ports, so that RB1-RB5 can learn the TRILL route from each other.
- The Te0/4 ports of RB1-RB2 and the Te0/3 ports of RB3-RB5 are configured as ACCESS-type TRILL ports for connecting to a common L2 network or terminal device to allow for the access of the original data packets to the TRILL network.
- The Te0/1~Te0/3 ports of RB1-RB2 act as DRB ports for their respective links.

### Network Topology

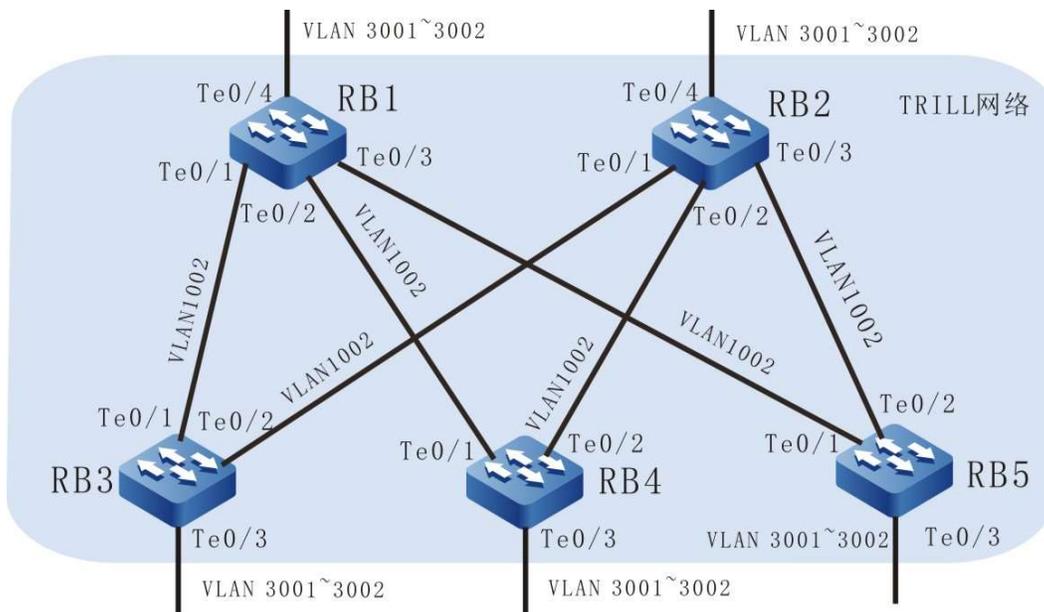


Figure 1-6 Configuring TRILL Network Topology

### Configuration Steps

Step 1: Configure the TRILL function for RB1-RB5.

Refer to the configurations of step 1 to step 4 of configuring the basic functions of TRILL.  
(Omitted)

Step 2: Configure the TRILL trunk ports of RB1-RB2 as the DRBs for their respective links.

#Configure the DRB priorities of the ports Te0/1-Te0/3 of RB1.

```
RB1(config)#interface tengigabitethernet 0/1
RB1(config-if-tengigabitethernet0/1)#trill drb-priority 127
```

```
RB1(config-if-tengigabitethernet0/1)#exit
RB1(config)#interface tengigabitethernet 0/2
RB1(config-if-tengigabitethernet0/2)#trill drb-priority 127
RB1(config-if-tengigabitethernet0/2)#exit
RB1(config)#interface tengigabitethernet 0/3
RB1(config-if-tengigabitethernet0/3)#trill drb-priority 127
RB1(config-if-tengigabitethernet0/3)#exit
```

#Configure the DRB priorities of the ports Te0/1-Te0/3 of RB2.

```
RB2(config)#interface tengigabitethernet 0/1
RB2(config-if-tengigabitethernet0/1)#trill drb-priority 127
RB2(config-if-tengigabitethernet0/1)#exit
RB2(config)#interface tengigabitethernet 0/2
RB2(config-if-tengigabitethernet0/2)#trill drb-priority 127
RB2(config-if-tengigabitethernet0/2)#exit
RB2(config)#interface tengigabitethernet 0/3
RB2(config-if-tengigabitethernet0/3)#trill drb-priority 127
RB2(config-if-tengigabitethernet0/3)#exit
```

Step 3: Check the results.

#View the DRB state of the port Te0/1 of RB1.

```
RB1#show trill interface tengigabitethernet 0/1
interface tengigabitethernet0/1: TRILL enabled
  Network Type: Broadcast
  Local circuit ID: 30
  Extended Local circuit ID: 1
  Local SNPA: 0001.7aee.820a
  Port Priority: 127
  Number of active adjacencies: 1
  Port State: DRB
  Port Type: TRUNK
  Link Running Mode: Bypass
  Desired Designated Vlan: 1002
  Designated Vlan: 1002
  Wide Metric: 20000
  DRB: 0001.7aee.820a.1A(self)
  DRB port id: 1
  DRB SNPA: 0001.7aee.820a
  Hello interval: 10 s
  Hello holding multiplier: 3
  CSNP interval: 10 s
  LSP TX interval: 33 ms
  LSP ReTransmit interval: 5 s
  Enabled VLAN:
    1002
  Announcing VLAN:
    1002
  Self 0001.7aee.820a AF VLAN:
    [none]
  Neighbor 0001.7aee.820c AF VLAN:
    [none]
```

#View the DRB state of the port Te0/2 of RB1.

```
RB1#show trill interface tengigabitethernet 0/2
interface tengigabitethernet0/2: TRILL enabled
  Network Type: Broadcast
  Local circuit ID: 31
  Extended Local circuit ID: 2
```

```
Local SNPA: 0001.7ace.820a
Port Priority: 127
Number of active adjacencies: 1
Port State: DRB
Port Type: TRUNK
Link Running Mode: Bypass
Desired Designated Vlan: 1002
Designated Vlan: 1002
Wide Metric: 20000
DRB: 0001.7ace.820a.1B(self)
DRB port id: 1
DRB SNPA: 0001.7ace.820a
Hello interval: 10 s
Hello holding multiplier: 3
CSNP interval: 10 s
LSP TX interval: 33 ms
LSP ReTransmit interval: 5 s
Enabled VLAN:
  1002
Announcing VLAN:
  1002
Self 0001.7ace.820a AF VLAN:
[none]
Neighbor 0001.7ace.820d AF VLAN:
[none]
```

#View the DRB state of the port Te0/3 of RB1.

```
RB1#show trill interface tengigabitethernet 0/3
interface tengigabitethernet0/3: TRILL enabled
Network Type: Broadcast
Local circuit ID: 32
Extended Local circuit ID: 3
Local SNPA: 0001.7ace.820a
Port Priority: 127
Number of active adjacencies: 1
Port State: DRB
Port Type: TRUNK
Link Running Mode: Bypass
Desired Designated Vlan: 1002
Designated Vlan: 1002
Wide Metric: 20000
DRB: 0001.7ace.820a.1C(self)
DRB port id: 1
DRB SNPA: 0001.7ace.820a
Hello interval: 10 s
Hello holding multiplier: 3
CSNP interval: 10 s
LSP TX interval: 33 ms
LSP ReTransmit interval: 5 s
Enabled VLAN:
  1002
Announcing VLAN:
  1002
Self 0001.7ace.820a AF VLAN:
[none]
Neighbor 0001.7ace.820e AF VLAN:
[none]
```

#View the DRB state of the port Te0/1 of RB2.

```
RB2#show trill interface tengigabitethernet 0/1
interface tengigabitethernet0/1: TRILL enabled
Network Type: Broadcast
```

Local circuit ID: 30  
Extended Local circuit ID: 1  
Local SNPA: 0001.7ace.820b  
Port Priority: 127  
Number of active adjacencies: 1  
**Port State: DRB**  
Port Type: TRUNK  
Link Running Mode: Bypass  
Desired Designated Vlan: 1002  
Designated Vlan: 1002  
Wide Metric: 20000  
DRB: 0001.7ace.820b.1E (self)  
DRB port id: 1  
DRB SNPA: 0001.7ace.820b  
Hello interval: 10 s  
Hello holding multiplier: 3  
CSNP interval: 10 s  
LSP TX interval: 33 ms  
LSP ReTransmit interval: 5 s  
Enabled VLAN:  
1002  
Announcing VLAN:  
1002  
Self 0001.7ace.820a AF VLAN:  
[none]  
Neighbor 0001.7ace.820c AF VLAN:  
[none]

#View the DRB state of the port Te0/2 of RB2.

```
RB2#show trill interface tengigabitethernet 0/2
interface tengigabitethernet0/2: TRILL enabled
Network Type: Broadcast
Local circuit ID: 31
Extended Local circuit ID: 2
Local SNPA: 0001.7ace.820b
Port Priority: 127
Number of active adjacencies: 1
Port State: DRB
Port Type: TRUNK
Link Running Mode: Bypass
Desired Designated Vlan: 1002
Designated Vlan: 1002
Wide Metric: 20000
DRB: 0001.7ace.820b.1E (self)
DRB port id: 1
DRB SNPA: 0001.7ace.820b
Hello interval: 10 s
Hello holding multiplier: 3
CSNP interval: 10 s
LSP TX interval: 33 ms
LSP ReTransmit interval: 5 s
Enabled VLAN:
1002
Announcing VLAN:
1002
Self 0001.7ace.820a AF VLAN:
[none]
Neighbor 0001.7ace.820d AF VLAN:
[none]
```

#View the DRB state of the port Te0/3 of RB2.

```

RB2#show trill interface tengigabitethernet 0/3
interface tengigabitethernet0/3: TRILL enabled
Network Type: Broadcast
Local circuit ID: 32
Extended Local circuit ID: 3
Local SNPA: 0001.7aee.820b
Port Priority: 127
Number of active adjacencies: 1
Port State: DRB
Port Type: TRUNK
Link Running Mode: Bypass
Desired Designated Vlan: 1002
Designated Vlan: 1002
Wide Metric: 20000
DRB: 0001.7aee.820b.1E (self)
DRB port id: 1
DRB SNPA: 0001.7aee.820b
Hello interval: 10 s
Hello holding multiplier: 3
CSNP interval: 10 s
LSP TX interval: 33 ms
LSP ReTransmit interval: 5 s
Enabled VLAN:
  1002
Announcing VLAN:
  1002
Self 0001.7aee.820a AF VLAN:
[none]
Neighbor 0001.7aee.820e AF VLAN:
[none]

```

### 125.4.3 Configure Distribution Tree Root Resolution for TRILL

#### Network Requirements

- TRILL is enabled for RB1-RB5 globally.
- Te0/1-Te0/3 ports of RB1-RB2 and Te0/1-Te0/2 ports of RB3-RB5 are configured as Trunk type TRILL ports, so that RB1-RB5 can learn the TRILL route from each other.
- The Te0/4 ports of RB1-RB2 and the Te0/3 ports of RB3-RB5 are configured as ACCESS-type TRILL ports for connecting to a common L2 network or terminal device to allow for the access of the original data packets to the TRILL network.
- RB1 and RB2 act as the roots of the two distribution trees in the TRILL network, respectively, and the root priorities decrease sequentially.

#### Network Topology

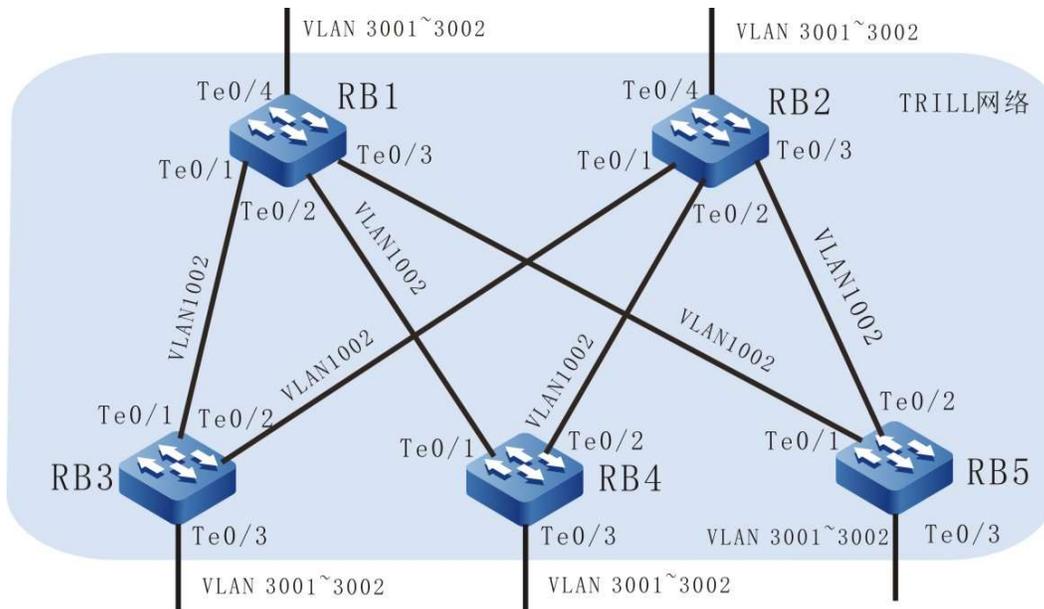


Figure 125-6 Configuring TRILL Network Topology

### Configuration Steps

Step 1: Configure the TRILL function for RB1-RB5.

Refer to the configurations of step 1 to step 4 of configuring the basic functions of TRILL.  
(Omitted)

Step 2: Configure the priorities of TRILL distribution tree roots for RB1-RB2 as 60000 and 50000, respectively, with RB1-RB5 configuring the number of distribution trees that native RB desires to compute in the entire network as 2.

#Configure the root priority of RB1 as 6000, and the number of distribution trees that native RB desires to compute in the entire network as 2.

```
RB1#configure terminal
RB1(config)#trill
RB1(config-trill)#nickname 0x0001 root-priority 60000
RB1(config-trill)#dtrees number-to-compute 2
RB1(config-trill)#exit
```

#Configure the root priority of RB2 as 5000, and the number of distribution trees that native RB desires to compute in the entire network as 2.

```
RB2#configure terminal
RB2(config)#trill
RB2(config-trill)#nickname 0x0002 root-priority 50000
RB2(config-trill)#dtrees number-to-compute 2
RB2(config-trill)#exit
```

#Configure the number of distribution trees that RB of RB3 desires to compute in the entire network as 2.

```
RB3#configure terminal
RB3(config)#trill
RB3(config-trill)#dtrees number-to-compute 2
RB3(config-trill)#exit
```

#Configure the number of distribution trees that RB of RB4 desires to compute in the entire network as 2.

```
RB4#configure terminal
RB4(config)#trill
RB4(config-trill)#dtrees number-to-compute 2
RB4(config-trill)#exit
```

#Configure the number of distribution trees that RB of RB5 desires to compute in the entire network as 2.

```
RB5#configure terminal
RB5(config)#trill
RB5(config-trill)#dtrees number-to-compute 2
RB5(config-trill)#exit
```

Step 3: Check the results.

#View the multicast route information of all distribution trees on RB1.

```
BR1#show trill multicast-route
Rbidge with highest priority tree root is 0x0001. LSP ID is 0001.7aee.820a.00-00

Dtree-number D-Tree_Name D-tree-system-id Hop-count
02 0x0002 0001.7aee.820b 002 Dtree to use
Adj_Nickname Adj_System_id Interface SNPA
0x0003 0001.7aee.820c tengigabitethernet0/1 0001.7aee.820c
0x0004 0001.7aee.820d tengigabitethernet0/2 0001.7aee.820d
0x0005 0001.7aee.820e tengigabitethernet0/3 0001.7aee.820e
Dtree-number D-Tree_Name D-tree-system-id Hop-count
01 0x0001 0001.7aee.820a 002 Dtree to use
Adj_Nickname Adj_System_id Interface SNPA
0x0003 0001.7aee.820c tengigabitethernet0/1 0001.7aee.820c
0x0004 0001.7aee.820d tengigabitethernet0/2 0001.7aee.820d
0x0005 0001.7aee.820e tengigabitethernet0/3 0001.7aee.820e
```

#View information of all the distribution trees on RB1.

```
RB1#show trill dtrees
DTree Number: 2
Root nickname: 0x0002 System ID: 0001.7aee.820b
Distance to Root: 40000
Dtree state: USE , Nexthop Valid
Number of vlans: 1
List of vlans:
[3001]
DTree Number: 1
Root nickname: 0x0001 System ID: 0001.7aee.820a
Distance to Root: 0
Dtree state: USE , Nexthop Valid
Number of vlans: 1
List of vlans:
[3002]
```

#View the multicast route information of all distribution trees on RB2.

```
BR2#show trill multicast-route
```

Rbidge with highest priority tree root is 0x0001. LSP ID is 0001.7ace.820a.00-00

```
Dtree-number D-Tree_Name D-tree-system-id Hop-count
02 0x0002 0001.7ace.820b 002 Dtree to use
Adj_Nickname Adj_System_id Interface SNPA
0x0003 0001.7ace.820c tengigabitethernet0/1 0001.7ace.820c
0x0004 0001.7ace.820d tengigabitethernet0/2 0001.7ace.820d
0x0005 0001.7ace.820e tengigabitethernet0/3 0001.7ace.820e
Dtree-number D-Tree_Name D-tree-system-id Hop-count
01 0x0001 0001.7ace.820a 002 Dtree to use
Adj_Nickname Adj_System_id Interface SNPA
0x0003 0001.7ace.820c tengigabitethernet0/1 0001.7ace.820c
0x0004 0001.7ace.820d tengigabitethernet0/2 0001.7ace.820d
0x0005 0001.7ace.820e tengigabitethernet0/3 0001.7ace.820e
```

### #View information of all the distribution trees on RB2.

```
RB2#show trill dtrees
DTree Number: 2
Root nickname: 0x0002 System ID: 0001.7ace.820b
Distance to Root: 0
Dtree state: USE , Nexthop Valid
Number of vlans: 1
List of vlans:
[3001]
DTree Number: 1
Root nickname: 0x0001 System ID: 0001.7ace.820a
Distance to Root: 40000
Dtree state: USE , Nexthop Valid
Number of vlans: 1
List of vlans:
[3002]
```

### #View the multicast route information of all distribution trees on RB3.

```
BR3#show trill multicast-route
Rbidge with highest priority tree root is 0x0001. LSP ID is 0001.7ace.820a.00-00
Dtree-number D-Tree_Name D-tree-system-id Hop-count
02 0x0002 0001.7ace.820b 002 Dtree to use
Adj_Nickname Adj_System_id Interface SNPA
0x0001 0001.7ace.820a tengigabitethernet0/1 0001.7ace.820a
0x0002 0001.7ace.820b tengigabitethernet0/2 0001.7ace.820b
Dtree-number D-Tree_Name D-tree-system-id Hop-count
01 0x0001 0001.7ace.820a 002 Dtree to use
Adj_Nickname Adj_System_id Interface SNPA
0x0001 0001.7ace.820a tengigabitethernet0/1 0001.7ace.820a
0x0002 0001.7ace.820b tengigabitethernet0/2 0001.7ace.820b
```

### #View information of all the distribution trees on RB3.

```
RB3#show trill dtrees
DTree Number: 2
Root nickname: 0x0002 System ID: 0001.7ace.820b
Distance to Root: 20000
Dtree state: USE , Nexthop Valid
Number of vlans: 1
List of vlans:
[3001]
DTree Number: 1
Root nickname: 0x0001 System ID: 0001.7ace.820a
Distance to Root: 20000
Dtree state: USE , Nexthop Valid
```

Number of vlans: 1  
List of vlans:  
[3002]

### #View the multicast route information of all distribution trees on RB4.

```
BR4#show trill multicast-route
Rbidge with highest priority tree root is 0x0001. LSP ID is 0001.7aee.820a.00-00

Dtree-number D-Tree_Name D-tree-system-id Hop-count
  02 0x0002 0001.7aee.820b 002 Dtree to use
  Adj_Nickname Adj_System_id Interface SNPA
  0x0001 0001.7aee.820a tengigabitethernet0/1 00:01:7a:ee:82:0a
  0x0002 0001.7aee.820b tengigabitethernet0/2 0001.7aee.820b
Dtree-number D-Tree_Name D-tree-system-id Hop-count
  01 0x0001 0001.7aee.820a 002 Dtree to use
  Adj_Nickname Adj_System_id Interface SNPA
  0x0001 0001.7aee.820a tengigabitethernet0/1 0001.7aee.820a
  0x0002 0001.7aee.820b tengigabitethernet0/2 0001.7aee.820b
```

### #View information of all the distribution trees on RB4.

```
RB4#show trill dtrees
DTree Number: 2
Root nickname: 0x0002 System ID: 0001.7aee.820b
Distance to Root: 20000
Dtree state: USE , Nexthop Valid
Number of vlans: 1
List of vlans:
[3001]
DTree Number: 1
Root nickname: 0x0001 System ID: 0001.7aee.820a
Distance to Root: 20000
Dtree state: USE , Nexthop Valid
Number of vlans: 1
List of vlans:
[3002]
```

### #View the multicast route information of all distribution trees on RB5.

```
BR5#show trill multicast-route
Rbidge with highest priority tree root is 0x0001. LSP ID is 0001.7aee.820a.00-00

Dtree-number D-Tree_Name D-tree-system-id Hop-count
  02 0x0002 0001.7aee.820b 002 Dtree to use
  Adj_Nickname Adj_System_id Interface SNPA
  0x0001 0001.7aee.820a tengigabitethernet0/1 0001.7aee.820a
  0x0002 0001.7aee.820b tengigabitethernet0/2 0001.7aee.820b
Dtree-number D-Tree_Name D-tree-system-id Hop-count
  01 0x0001 0001.7aee.820a 002 Dtree to use
  Adj_Nickname Adj_System_id Interface SNPA
  0x0001 0001.7aee.820a tengigabitethernet0/1 0001.7aee.820a
  0x0002 0001.7aee.820b tengigabitethernet0/2 0001.7aee.820b
```

### #View information of all the distribution trees on RB5.

```
RB5#show trill dtrees
DTree Number: 2
Root nickname: 0x0002 System ID: 0001.7aee.820b
Distance to Root: 20000
Dtree state: USE , Nexthop Valid
Number of vlans: 1
List of vlans:
[3001]
```

DTree Number: 1  
 Root nickname: 0x0001 System ID: 0001.7acc.820a  
 Distance to Root: 20000  
 Dtree state: USE , Nexthop Valid  
 Number of vlans: 1  
 List of vlans:  
 [3002]

## 125.4.4 Configure AVF VLAN Selection of TRILL

### Network Requirements

- TRILL is enabled for RB1-RB5 globally.
- Te0/1-Te0/3 ports of RB1-RB2 and Te0/1-Te0/2 ports of RB3-RB5 are configured as Trunk type TRILL ports, so that RB1-RB5 can learn the TRILL route from each other.
- The Te0/4 ports of RB1-RB2 and the Te0/3 ports of RB3-RB5 are configured as ACCESS-type TRILL ports for connecting to a common L2 network or terminal device to allow for the access of the original data packets to the TRILL network.
- AVF of RB3 acts as service VLAN 3001, and AVF of RB4 acts as service VLAN 3002.

### Network Topology

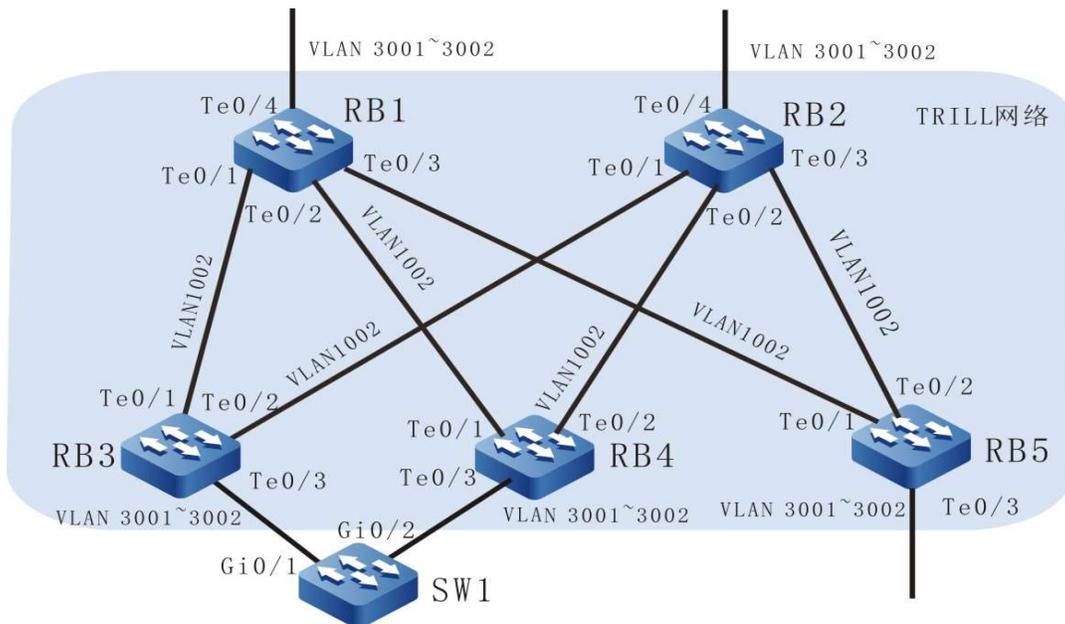


Figure 125-7 Configuring TRILL Network Topology

### Configuration Steps

Step 1: Configure the TRILL function for RB1-RB5. (Omitted)

Refer to the configurations of step 1 to step 4 of configuring the basic functions of TRILL.  
(Omitted)

Step 2: Configure the Gi0/1~Gi0/2 ports of SW1 to join vlan3001-vlan3002 in Trunk mode.  
(Omitted)

Step 3: Configure the AVFs of RB3-RB4, where RB3 acts as the AVF of VLAN3001 and RB4 acts the AVF of VLAN3002.

#Configure the Te0/3 port of RB3 as the DRB of the link to which it belongs, and designate the AVF of the service VLAN3002 as RB4.

```
RB3(config)#interface tengigabitethernet 0/3
RB3(config-if-tengigabitethernet0/3)#trill drb-priority 127
RB3(config-if-tengigabitethernet0/3)#trill vlan-forwarder nickname 0x0004 vlan 3002
RB3(config-if-tengigabitethernet0/3)#exit
```

#No need to configure RB4.

Step 4: Check the results.

#View the AVF VLAN on RB3.

```
RB3#show trill vlan-forwarder
AF VLAN on interface tengigabitethernet0/1
[none]
AF VLAN on interface tengigabitethernet0/2
[none]
AF VLAN on interface tengigabitethernet0/3
[3001]
```

#View the AVF VLAN on RB4.

```
RB4#show trill vlan-forwarder
AF VLAN on interface tengigabitethernet0/1
[none]
AF VLAN on interface tengigabitethernet0/2
[none]
AF VLAN on interface tengigabitethernet0/3
[3002]
```

## 125.4.5 Configure Load Balancing for TRILL

### Network Requirements

- TRILL is enabled for RB1-RB5 globally.
- Te0/1-Te0/3 ports of RB1-RB2 and Te0/1-Te0/2 ports of RB3-RB5 are configured as Trunk type TRILL ports, so that RB1-RB5 can learn the TRILL route from each other.
- The Te0/4 ports of RB1-RB2 and the Te0/3 ports of RB3-RB5 are configured as ACCESS-type TRILL ports for connecting to a common L2 network or terminal device to allow for the access of the original data packets to the TRILL network.

- RB1-RB5 can each generate a load balancing route for TRILL known unicast.

### Network Topology

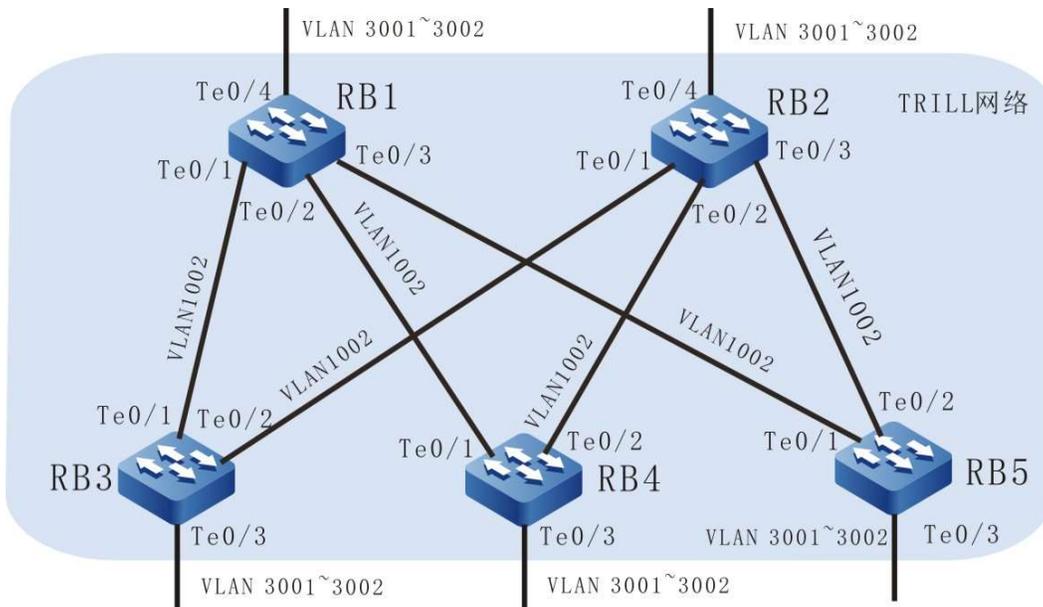


Figure 125-8 Configuring TRILL Network Topology

### Configuration Steps

Step 1: Configure the TRILL function for RB1-RB5. (Omitted)

Refer to the configurations of step 1 to step 4 of configuring the basic functions of TRILL. (Omitted)

Step 2: Check the results.

View the information of the trill unicast load balancing route via show trill unicast-route.

#View the information of the unicast load balancing route of RB1.

```
RB1#show trill unicast-route
TRILL Unicast Forwarding Database
Eg_Nick  Eg_SysId  Metric HopCnt NH_Nick  NH_SysId  Interface      SNPA
0x0002  0001.7ace.820b 40000 002 0x0003  0001.7ace.820c tengigabitethernet0/1 0001.7ace.820c
                                0x0004  0001.7ace.820d tengigabitethernet0/2 0001.7ace.820d
                                0x0005  0001.7ace.820e tengigabitethernet0/3 0001.7ace.820e
0x0003  0001.7ace.820c 20000 001 0x0003  0001.7ace.820c tengigabitethernet0/1 0001.7ace.820c
0x0004  0001.7ace.820d 20000 001 0x0004  0001.7ace.820d tengigabitethernet0/2 0001.7ace.820d
0x0005  0001.7ace.820e 20000 001 0x0005  0001.7ace.820e tengigabitethernet0/3 0001.7ace.820e
```

#View the information of the unicast load balancing route of RB2.

```
RB2#show trill unicast-route
TRILL Unicast Forwarding Database
```

Eg_Nick	Eg_SysId	Metric	HopCnt	NH_Nick	NH_SysId	Interface	SNPA
0x0001	0001.7ace.820a	40000	002	0x0003	0001.7ace.820c	tengigabitethernet0/1	0001.7ace.820c
				0x0004	0001.7ace.820d	tengigabitethernet0/2	0001.7ace.820d
				0x0005	0001.7ace.820e	tengigabitethernet0/3	0001.7ace.820e
0x0003	0001.7ace.820c	20000	001	0x0003	0001.7ace.820c	tengigabitethernet0/1	0001.7ace.820c
0x0004	0001.7ace.820d	20000	001	0x0004	0001.7ace.820d	tengigabitethernet0/2	0001.7ace.820d
0x0005	0001.7ace.820e	20000	001	0x0005	0001.7ace.820e	tengigabitethernet0/3	0001.7ace.820e

#View the information of the unicast load balancing route of RB3.

```
RB3#show trill unicast-route
TRILL Unicast Forwarding Database
```

Eg_Nick	Eg_SysId	Metric	HopCnt	NH_Nick	NH_SysId	Interface	SNPA
0x0001	0001.7ace.820a	20000	001	0x0001	0001.7ace.820a	tengigabitethernet0/1	0001.7ace.820a
0x0002	0001.7ace.820b	20000	001	0x0002	0001.7ace.820b	tengigabitethernet0/2	0001.7ace.820b
0x0004	0001.7ace.820d	40000	002	0x0001	0001.7ace.820a	tengigabitethernet0/1	0001.7ace.820a
				0x0002	0001.7ace.820b	tengigabitethernet0/2	0001.7ace.820b
0x0005	0001.7ace.820e	40000	002	0x0001	0001.7ace.820a	tengigabitethernet0/1	0001.7ace.820a
				0x0002	0001.7ace.820b	tengigabitethernet0/2	0001.7ace.820b

#View the information of the unicast load balancing route of RB4.

```
RB4#show trill unicast-route
TRILL Unicast Forwarding Database
```

Eg_Nick	Eg_SysId	Metric	HopCnt	NH_Nick	NH_SysId	Interface	SNPA
0x0001	0001.7ace.820a	20000	001	0x0001	0001.7ace.820a	tengigabitethernet0/1	0001.7ace.820a
0x0002	0001.7ace.820b	20000	001	0x0002	0001.7ace.820b	tengigabitethernet0/2	0001.7ace.820b
0x0003	0001.7ace.820c	40000	002	0x0001	0001.7ace.820a	tengigabitethernet0/1	0001.7ace.820a
				0x0002	0001.7ace.820b	tengigabitethernet0/2	0001.7ace.820b
0x0005	0001.7ace.820e	40000	002	0x0001	0001.7ace.820a	tengigabitethernet0/1	0001.7ace.820a
				0x0002	0001.7ace.820b	tengigabitethernet0/2	0001.7ace.820b

#View the information of the unicast load balancing route of RB5.

```
RB5#show trill unicast-route
TRILL Unicast Forwarding Database
```

Eg_Nick	Eg_SysId	Metric	HopCnt	NH_Nick	NH_SysId	Interface	SNPA
0x0001	0001.7ace.820a	20000	001	0x0001	0001.7ace.820a	tengigabitethernet0/1	0001.7ace.820a
0x0002	0001.7ace.820b	20000	001	0x0002	0001.7ace.820b	tengigabitethernet0/2	0001.7ace.820b
0x0003	0001.7ace.820c	40000	002	0x0001	0001.7ace.820a	tengigabitethernet0/1	0001.7ace.820a
				0x0002	0001.7ace.820b	tengigabitethernet0/2	0001.7ace.820b
0x0004	0001.7ace.820d	40000	002	0x0001	0001.7ace.820a	tengigabitethernet0/1	0001.7ace.820a
				0x0002	0001.7ace.820b	tengigabitethernet0/2	0001.7ace.820b

# 126 VXLAN

---

## 126.1 Overview

### 126.1.1 Background

In order for high reliability and redundant deployment, most enterprise networks and their data centers at present span multiple physical sites in different physical locations, and similar services are deployed at these sites. To consolidate data center resources and reduce management costs, it is common to virtualize data center resources. Data center virtualization has three main aspects: network virtualization, storage virtualization, and server virtualization. In server virtualization, dedicated virtualization software is used to virtualize multiple virtual machines on one physical server. Each virtual machine runs independently and has its own operating system, applications, and virtual hardware environment. In order for dynamic allocation and management of resources between sites, the virtual machines need to be freely migratable between the data centers. Since the virtual machine migration process is transparent to users with the IP address unable to be varied, this requests that before and after migration of the virtual machines the network is one L2 network, so there must be L2 network interconnection between sites in different locations.

VXLAN is one "MAC in IP" technology that is used to implement large two-layer internetworking based on the IP core network. VXLAN only maintains the MAC address and forwarding information on the edge devices of the site, without changing the internal network and core network structures of the site.

Using VXLAN as the large two-layer internetworking technology has the following advantages:

- VXLAN encapsulates the data packets sent by the virtual machine into UDP and uses the IP/MAC address of the physical network as the outer header for encapsulating, with only encapsulated parameters represented for the network. Therefore, the requirements of the large two-layer network for MAC address specification are greatly lowered. Except for the edge devices of the VXLAN network, other devices on the network have no need to identify MAC addresses of virtual machines, reducing the MAC address learning pressure for the devices and improving device performance.
- VXLAN introduces user ID similar to VLAN ID, called VXLAN network ID VNI, which consists of 24 bits and supports up to 16,777,215 VXLAN segments, thereby satisfying numerous user IDs.
- By using MAC in UDP encapsulation to extend the two-layer network, the physical network and the virtual network are decoupled. Tenants can plan their own virtual

networks without considering the restrictions on physical network IP addresses and broadcast domains, allowing for greatly reduced difficulty in network management.

## **126.1.2 Basic Concepts**

### **Network Virtual Edge Node**

NVE (Network Virtualization Edge) is a network entity that implements network virtualization. Once packets are encapsulated and converted by the NVE network entity, a virtual VXLAN network can be established between NVEs based on the L3 basic network.

### **VXLAN Tunnel End Point**

VTEP (VXLAN Tunnel End Point) is a switch device at the edge of a site. It functions as a L2 device on the site network and a L3 device on the core network. It primarily provides L2 interconnection between site networks. It completes packet encapsulation from the site network to the core network and packet decapsulation from the core network to the site network.

Core network port: A L3 port, i.e., Network Port, for the edge device to connect to the core network.

Site internal port: A L2 port, i.e., Internal Port, for the edge device to connect to site internal devices.

### **VXLAN Session**

VXLAN Session is a valid forwarding instance formed between VTEPs by establishing a VXLAN tunnel via manual configuration or protocol negotiation and associating it with an VXLAN instance. Data can be forwarded only after the VXLAN session is valid.

### **EVPN**

EVPN (Ethernet Virtual Private Network) is one L2 VPN technology. EVPN technology uses extended MP-BGP to spread the host information in the user network among sites, and uses the control plane instead of the data plane to complete cross-site MAC address learning in the user network.

VXLAN itself is one data encapsulation protocol and does not define a control plane. MAC addresses between sites are learned, using traditional traffic flooding on the data plane. The greatest disadvantage of this manner lies in that the data center carrying network has a large amount of flooding traffic. To address this issue, VXLAN introduces EVPN as the control plane to exchange BGP EVPN routes between VTEPs to implement features such as automatic VTEP discovery and mutual advertising of host information, thereby avoiding unnecessary data traffic flooding.

### 126.1.3 Protocol Specification

- RFC7348: Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks.
- RFC 7432: BGP MPLS-Based Ethernet VPN
- RFC 8365--A Network Virtualization Overlay Solution Using Ethernet VPN (EVPN)
- draft-ietf-bess-evpn-inter-subnet-forwarding-05
- draft-ietf-bess-evpn-prefix-advertisement-11
- draft-malhotra-bess-evpn-irb-extended-mobility-03

### 126.2 VXLAN Function Configuration

Table 126-1 VXLAN Function Configuration List

Configuration Task	
Configure basic functions of VXLAN	Configure VXLAN instance
	Configure VXLAN instance description information
	Configure to add the port into the VXLAN instance
	Configure VXLAN L3 interface
	Configure NVE
	Configure to enable ARP host advertising
	Configure to enable ARP broadcast suppression
Configure static VXLAN	Configure VXLAN static headend replication list
Configure EVPN VXLAN	Configure NVE to enable EVPN
	Configure EVPN attributes of the VXLAN instance
	Configure EVPN attributes of the VRF instance (optional)

Configuration Task	
	Configure BGP to enable EVPN
	Configure BGP neighbor policy (optional)
	Configure VXLAN route map (optional)

## 126.2.1 Configure VXLAN instance

### Configuration Condition

None

### Configure VXLAN Instance

Each VXLAN instance is one independent working interval, separated by VNID, so that different VXLAN instances cannot communicate with each other, while VXLAN instances that are the same can communicate with each other, the device supports the configuration of up to 4096 VXLAN instances.

Table 126-2 Configuring VXLAN Instance

Step	Command	Description
Global configuration mode	<b>configure terminal</b>	-
VXLAN configuration mode	<b>vxlan vxlan-id</b>	Mandatory By default, no VXLAN is created
Configure VXLAN VNID	<b>vxlan vnid vnid</b>	By default, no configuring is performed

### Note

- VNID of the VXLAN instance must be configured first, otherwise other service configurations will not take effect.

## Configure VXLAN Instance Description Information

For the convenience of memorization and management, VXLAN description information can be configured according to VXLAN service type, function, connection status etc.

Table 2-3 Configuring VXLAN Description Information

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter VXLAN configuration mode	<b>vxlan</b> <i>vxlan-id</i>	Mandatory You can configure VXLAN description information only after entering the VXLAN configuration mode
Configure VXLAN description information	<b>description</b> <i>description-name</i>	Optional By default, there is no description of VXLAN

## VXLAN Instance Service Access

VXLAN does not contain any service access points when initially created. By using different access manners, virtual machines can be connected to the VXLAN network to implement VXLAN network forwarding for virtual machine services. The access modes are as follows:

Table 126-3 Configuring Service Point Mode

Mode	Description
default	Allow the port to receive all packets, regardless of whether the packets carry VLAN tags or not.  Regardless of the VXLAN encapsulation of the original packets or the decapsulation of the VXLAN packets, this type of port will not perform any VLAN Tag processing on the original packets, including adding, replacing or stripping.

Mode	Description
untag	<p>This type of port only receives packets without VLAN tags</p> <p>This mode supports both L2 forwarding and L3 forwarding</p>
dot1q	<p>This type of port only receives packets with VLAN tags with the outer VLAN tag matching the designated VLAN tag;</p> <p>This type of port will strip the outermost VLAN tag upon VXLAN encapsulation on the original packets;</p> <p>It will add the designated VLAN Tag before forwarding upon decapsulation of VXLAN packets.</p> <p>This mode needs to add the physical port into the corresponding VLAN, and the global VLAN needs to be created</p> <p>This mode supports both L2 forwarding and L3 forwarding</p>

The VXLAN instance does not contain any service access points when initially created, so you need to manually configure the following.

Table 126-4 Configuring Service Point

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure port mode	<b>interface tengigabitethernet 0/1</b>	<p>Mandatory</p> <p>You can configure to add the port into the VXLAN instance only after entering the port mode. Aggregation ports are supported</p>
Configure VXLAN Instance access method	<b>vxlan vxlan-id encapsulation { vlan vlan-id   untag   default }</b>	<p>Mandatory</p> <p>By default, no port is added into VXLAN</p>

Step	Command	Description
		After the port is added into VXLAN, the VXLAN function will take effect on the port

## Note

- When the access modes are untag and default, the same port cannot be added to multiple VXLAN instances at the same time.
- When the access mode is dot1q, the VXLAN access port needs to be configured as tag access

### Configure VXLAN L3 Interface

When enabling the L3 VXLAN function, you must configure the VXLAN L3 interface and designate the IP.

Table 126-5 Configuring VLAN Interface

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the VXLAN interface	<b>interface vxlan</b> <i>vxlan-id</i>	Mandatory By default, no VXLAN interface is configured. When enabling the L3 VXLAN function, you must perform configuring.
Configure VXLAN interface to associate with VRF	<b>ip vrf forwarding</b> <i>vrf-name</i>	Optional By default, the VXLAN interface is not associated with VRF
Configure IP address for VXLAN interface	<b>ip address</b> <i>X.X.X.X</i>	Mandatory

Step	Command	Description
		By default, no IP address is configured for the VXLAN interface. When enabling the L3 VXLAN function, you must perform configuring.

### Configure NVE

NVE (Network Virtualization Edge) is a network entity that implements network virtualization. Once packets are encapsulated and converted by the NVE network entity, a virtual VXLAN network can be established between NVEs based on the L3 basic network.

Table 126-6 Configuring NVE

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Create NVE interface	<b>interface nve</b> <i>nve-number</i>	Mandatory By default, no NVE interface is created on the device
Configure MAC address	<b>mac-address</b> <i>mac</i>	Optional By default, no MAC address is configured on the NVE interface
Configure source IP address	<b>source</b> <i>ip-address</i>	Mandatory By default, no VTEP IP address is configured on the NVE interface

### Configure to Enable ARP Host Advertising

After the ARP host advertising function is enabled under the VXLAN instance, the ARP request packets, ARP response packets, and gratuitous ARP packets received on the user-side port will generate the local ARP host table and advertise to the EVPN route, and then to neighbors via the BGP EVPN protocol,

thereby allowing for route learning between VTEPs and installation of the ARP broadcast suppression table.

Table 126-7 Enabling ARP Host Advertising

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter VXLAN configuration mode	<b>vxlan vxlan-id</b>	Mandatory
Configure to enable ARP host advertising	<b>arp host advertise</b>	Mandatory By default, the state is not enabled

#### Configure to Enable ARP Broadcast Suppression

After VXLAN enables the ARP broadcast suppression function and the ARP broadcast request packet is received on the user-side port, the request destination IP is used to query the ARP broadcast suppression table. For the ARP broadcast request packet that matches the suppression table, it can be subjected to proxy response or forwarded to unicast; for the ARP broadcast request packet that mismatches the suppression table, it can be broadcast or discarded.

After the ARP broadcast suppression function is enabled, the number of broadcast packets in the VXLAN domain can be reduced.

Table 126-8 Enabling ARP Broadcast Suppression

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Enter VXLAN configuration mode	<b>vxlan vxlan-id</b>	Mandatory
Configure to enable the ARP broadcast suppression function	<b>arp suppression</b>	Mandatory By default, the broadcast suppression function is disabled

Step	Command	Description
After configuring the match suppression table, performing unicast forwarding	<b>arp suppression unicast forward</b>	Optional By default, the ARP request packets that matches the suppression table undergo proxy response.
Configure the mismatch suppression table and perform discarding	<b>arp suppression mismatch discard</b>	Optional By default, the ARP request packet that mismatches the suppression table is broadcast.

## 126.2.2 Configure Static VXLAN Tunnel

### Configuration Condition

None

### Configure Static Headend Replication List for VXLAN Instance

The headend refers to the ingress node of the VXLAN tunnel, and the replication list refers to that when the ingress node of the VXLAN tunnel receives a BUM (Broadcast&Unknown-unicast&Multicast) packet, it will make multiple copies of the packet and send them to all VTEPs in the list. The headend replication list is the IP address list of the remote VTEPs that is used to direct the ingress node of the VXLAN tunnel to copy and send the BUM packet.

The headend replication list, usually called BUM VXLAN tunnel, uses the headend replication list source NVE interface to replicate the received BUM packet according to the VTEP list and send it to all VTEPs belonging to the same VNI.

Table 126-9 Configuring VXLAN Static Headend Replication List

Step	Command	Description
Global configuration mode	<b>configure terminal</b>	-

Step	Command	Description
NVE interface configuration mode	<b>interface nve</b> <i>nve-number</i>	Mandatory
Configure static headend replication list for designated VXLAN	<b>vxlan vxlan-id ingress-replication peer</b> { <i>ip-address</i>   <i>ipv6-address</i> }	Mandatory By default, no static headend replication list is configured

---

## Note

- Even if the source VTEP only corresponds to one remote VTEP, you need to execute this command to designate the corresponding VTEP address and configure the headend replication list.
- 

### 126.2.3 Configure EVPN VXLAN Tunnel

#### Configuration Condition

- Before configuring BGP EVPN method to deploy VXLAN services, ensure that:
  - The link layer protocol has been configured to ensure normal communication at the link layer.
  - Configure address of interface at network layer so that neighbor network nodes are reachable at the network layer.

#### Configure NVE to Enable EVPN Protocol

After NVE activates EVPN, automatic negotiation between VTEPs and automatic establishment of the VXLAN tunnel can be performed via the the BGP EVPN protocol.

Table 126-10 Configuring Dynamic VXLAN Tunnel

Step	Command	Description
Global configuration mode	<b>configure terminal</b>	-
NVE interface configuration mode	<b>interface nve</b> <i>nve-number</i>	Mandatory
Configure the designated VXLAN instance to associate with NVE	<b>vxlan</b> <i>vxlan-id</i>	Mandatory By default, no associating is performed
Configure the designated VXLAN instance to use EVPN to establish the headend replication list	<b>vxlan</b> <i>vxlan-id</i> <b>ingress-replication protocol bgp</b>	Optional By default, no designating is performed

### Configure EVPN Attributes of the VXLAN Instance

Rd is used to mark the EVPN routes generated by different VXLANs, isolating the different VXLANs; route-target is used to control the import and export of EVPN routes. When the VTEP initiates the EVPN route, it carries the Export RT attribute. When the VTEP decides which VXLAN to import the EVPN route into, the Export RT attribute carried by the route is used to match the Import RT of the local VXLAN.

Table 126-11 Configuring VXLAN EVPN Attribute

Step	Command	Description
Global configuration mode	<b>configure terminal</b>	-
VXLAN instance configuration mode	<b>vxlan</b> <i>vxlan-id</i>	Mandatory You can enter the EVPN configuration mode only when in

Step	Command	Description
		the VXLAN configuration mode
VXLAN EVPN configuration mode	<b>address-family evpn</b>	Mandatory You can configure VXLAN EVPN attributes only after entering the VXLAN EVPN configuration mode
Configure rd for VXLAN	<b>rd</b> <i>route-distinguisher</i>	Mandatory By default, RD for VXLAN is not configured
Configure route-target for VXLAN	<b>route-target</b> <b>[both   export   import]</b> { <i>ASN:nn</i>   <i>IP-address:nn</i> }	Mandatory By default, the Export and Import RT attributes of VXLAN are not configured

### Configure EVPN Attributes of the VRF Instance (Optional)

You need to configure the EVPN attributes of the VRF instance only when the distributed gateway is deployed, and you can skip this configuration for the centralized gateway deployment.

Table 126-12 Configuring EVPN Attributes of the VRF Instance

Step	Command	Description
Global configuration mode	<b>configure terminal</b>	-
Enter the VRF configuration mode	<b>ip vrf</b> <i>vrf-name</i>	Mandatory
Configure rd	<b>rd</b> <i>route-distinguisher</i>	Mandatory

Step	Command	Description
		By default, rd is not configured.
Configure L3VNID	<b>l3vnid</b> <i>vnid-number</i>	Mandatory  By default, L3VNID is not configured.
Enter the VRF EVPN address family configuration mode	<b>address-family evpn</b>	Mandatory
Configure route-target for VRF EVPN	<b>route-target [ both   export   import ]</b> { <i>ASN:nn</i>   <i>IP-address:nn</i> }	Mandatory  By default, the Import and Export attributes are not configured.
Associate VRF EVPN with the outbound routing policy	<b>export map</b> <i>route-map-name</i>	Optional  By default, VRF EVPN is not associated with the outbound routing policy
Associate VRF EVPN with the inbound routing policy	<b>import map</b> <i>route-map-name</i>	Optional  By default, VRF EVPN is not associated with the inbound routing policy

### Configure BGP to Enable EVPN

Enable EVPN capability for BGP to allow BGP to learn EVPN routing, creating the dynamic VXLAN tunnel, forming the VXLAN session, and adding to the forwarding table to guide VXLAN packet forwarding.

Table 126-13 Configuring BGP EVPN to Enable EVPN

Step	Command	Description
Global configuration mode	<b>configure terminal</b>	-
Enable the BGP protocol and enter the BGP configuration mode	<b>router bgp</b> <i>autonomous-system</i>	Mandatory By default, it is not enabled.
Configure BGP Neighbor	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>remote-as</b> <i>as-number</i>	Mandatory By default, no BGP neighbor is created.
Configure source address for TCP session of BGP neighbors	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>update-source</b> { <i>interface-name</i>   <i>ip-address</i> }	Optional By default, the TCP session automatically selects the address of the route's output interface as source address.
Enter the BGP EVPN configuration mode	<b>address-family l2vpn evpn</b>	Mandatory
Activate EVPN capability	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>activate</b>	Mandatory By default, it is not activated.
Configure EVPN reflector	<b>neighbor</b> { <i>neighbor-address</i>   <i>peer-group-name</i> } <b>route-reflector-client</b>	Optional By default, the reflector is not enabled
Enter the BGP IPv4 VRF configuration mode	<b>address-family ipv4 vrf</b> <i>vrf-name</i>	Optional
Configure to redistribute the VRF unicast route to EVPN	<b>advertise-l2vpn-evpn</b>	Optional

Step	Command	Description
to form a category 5 route		This configuration is only required for distributed gateway deployment.
Enter the BGP EVPN configuration mode	<b>address-family l2vpn evpn</b>	Mandatory
Configure not to change the as-path, med, and next-hop attribute values of the route when BGP advertises the route to neighbors or peer groups	<b>neighbor attribute-unchanged[ as-path   med   next-hop ]</b>	Optional This configuration is required only when an end-to-end cross-data center VXLAN network is deployed.

### Configure BGP Neighbor Policy (Optional)

By binding the route map to the BGP EVPN neighbors, you can effectively filter the routes received in the inbound direction that carry the designated VNI, or prevent advertising to the neighbors, certain routes that carry the designated VNI, in the outbound direction.

Table 126-14 Configuring BGP Neighbor EVPN Policy

Step	Command	Description
Global configuration mode	<b>configure terminal</b>	-
Enable the BGP protocol and enter the BGP configuration mode	<b>router bgp <i>autonomous-system</i></b>	Mandatory By default, BGP is disabled.
Enter the BGP EVPN configuration mode	<b>address-family l2vpn evpn</b>	Mandatory
Configure neighbors to apply the routing map in the inbound direction	<b>neighbor { <i>neighbor-address</i>   <i>peer-group</i></b>	Mandatory

Step	Command	Description
	<b><i>name</i> } route-map <i>rtmap-name</i> in</b>	By default, no route map is applied in the inbound direction
Configure neighbors to apply the routing map in the outbound direction	<b>neighbor { <i>neighbor-address</i>   <i>peer-group-name</i> } route-map <i>rtmap-name</i> out</b>	Mandatory By default, no route map is applied in the outbound direction

### Configure VXLAN Route Map (Optional)

When configuring the neighbor VXLAN policy, you need to bind the route map, and use the route map to acquire matches such as local VXLAN number and route next hop to control the inbound and outbound routes.

Table 126-15 Configuring VXLAN Route Map

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Create Routing Map	<b>route-map <i>map-name</i> [ { permit   deny } [ <i>seq-number</i> ] ]</b>	Mandatory By default, no routing map is created.
Match vxlan-id	<b>match vxlan <i>vxlan-id</i></b>	Optional By default, matching local VXLAN numbers is not performed

### 126.2.4VXLAN Monitoring and Maintaining

Table 126-16 VXLAN Monitoring and Maintaining

Command	Description
<b>clear arp host vxlan</b> [ all   vxlan-id [ip-address] ]	Clear the local ARP host information in the VXLAN instance
<b>show arp host vxlan</b> [ vxlan-id ]	View the local ARP host information in the VXLAN instance
<b>show arp suppression</b> [ vxlan vxlan-id ]	View the ARP broadcast suppression table in the VXLAN instance
<b>show bgp l2vpn evpn</b> { all   rd route-distinguisher   vxlan-id } { all-type   type { 2 [eth-tag-id:ip-addr-len:ip-address]   3 [eth-tag-id:mac-addr-len:mac-addr:ip-addr-len:ip-addr] }   5 [eth-tag-id:ip-addr-len:ip-addr] }	Show the routing information under MVPN address family of BGP
<b>show bgp l2vpn evpn conf</b>	Show EVPN related configuration information
<b>show bgp l2vpn evpn</b> {vxlan vxlan-id   vrf vrf-name}	Show EVPN VXLAN/VRF related information
<b>show bgp l2vpn evpn</b> { all   rd route-distinguisher [vxlan-id] } neighbors ip-address { advertised-routes   received-routes   routes } { all-type   type 2   type 3   type 5 }	Show the route information of the designated neighbor under the BGP EVPN address family
<b>show bgp l2vpn evpn vxlan-id statistic</b>	Show the route statistics of the designated VXLAN under the BGP EVPN address family
<b>show bgp l2vpn evpn summary</b>	Show BGP EVPN neighbor summary
<b>show vxlan vxlan-id config</b>	Show the configuration information of the designated VXLAN instance
<b>show vxlan vxlan-id instance</b>	Show the instance information of the designated VXLAN

Command	Description
<b>show vxlan vxlan-id internal</b>	Show the service access point of the designated VXLAN instance
<b>show vxlan vxlan-id session</b>	Show all session information associated with the designated VXLAN instance
<b>show vxlan config</b>	Show the global information of VXLAN
<b>show vxlan instance</b>	Show VXLAN instance information
<b>show vxlan internal [interface interface-num   interface link-aggregation link-aggregation-id ]</b>	Show the service access points of VXLAN
<b>show vxlan tunnel</b>	Show VXLAN tunnel information
<b>show vxlan session</b>	Show VXLAN session information

## 126.3 Typical Configuration Example of VXLAN

### 126.3.1 Configure Static VXLAN for Two-layer Intercommunication

#### Network Requirements

- Leaf1 and Leaf2 serve as VTEPs to create VXLAN instances.
- Leaf1 and Leaf2 establish static VXLAN tunnels through loopback interfaces.
- VMs in Server1 and Server2 on the same network segment can communicate with each other through the established VXLAN tunnel,

#### Network Topology

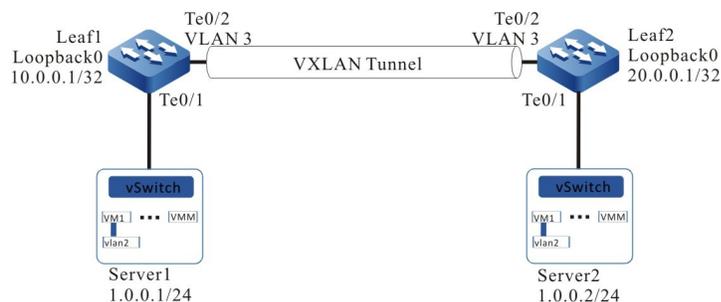


Figure 126-1 Network Topology for Configuring Static VXLAN for Two-layer Intercommunication

## Configuration Steps

Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configure IP addresses for the ports.

#Configure Leaf1.

```
Leaf1(config)#interface loopback 0
Leaf1(config-if-loopback0)#ip address 10.0.0.1 255.255.255.255
Leaf1(config-if-loopback0)#exit
Leaf1(config)#interface vlan 3
Leaf1(config-if-vlan3)#ip address 2.0.0.1 255.255.255.0
Leaf1(config-if-vlan3)#exit
```

#Configure Leaf2.

```
Leaf2(config)#interface loopback 0
Leaf2(config-if-loopback0)#ip address 20.0.0.1 255.255.255.255
Leaf2(config-if-loopback0)#exit
Leaf2(config)#interface vlan 3
Leaf2(config-if-vlan3)#ip address 2.0.0.2 255.255.255.0
Leaf2(config-if-vlan3)#exit
```

Step 3: Configure OSPF so that the routes of Loopback between devices are reachable from each other.

#Configure Leaf1.

```
Leaf1#configure terminal
Leaf1(config)#router ospf 100
Leaf1(config-ospf)#network 10.0.0.1 0.0.0.0 area 0
Leaf1(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Leaf1(config-ospf)#exit
```

#Configure Leaf2.

```
Leaf2#configure terminal
Leaf2(config)#router ospf 100
Leaf2(config-ospf)#network 20.0.0.1 0.0.0.0 area 0
Leaf2(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Leaf2(config-ospf)#exit
```

#View the routing table of Leaf1.

```

Leaf1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 2.0.0.0/24 is directly connected, 00:05:40, vlan3
C 127.0.0.0/8 is directly connected, 1d:21:38:36, lo0
C 10.0.0.1/32 is directly connected, 00:06:34, loopback0
O 20.0.0.1/32 [110/2] via 2.0.0.2, 00:00:05, vlan3

```

#### #View the routing table of Leaf2.

```

Leaf2#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 2.0.0.0/24 is directly connected, 00:06:43, vlan3
C 127.0.0.0/8 is directly connected, 1w3d:03:35:57, lo0
O 10.0.0.1/32 [110/2] via 2.0.0.1, 00:02:36, vlan3
C 20.0.0.1/32 is directly connected, 00:07:07, loopback0

```

It is indicated that both Leaf1 and Leaf2 have learned the route of the loopback interface of the peer end by running the OSPF protocol, making preparations for the next step of Leaf1 and Leaf2 establishing IBGP neighbors via the loopback interface.

Step 4: Configure VXLAN and associate VNID so that the ports of Leaf1 and Leaf2 are added into VXLAN.

#### #Configure Leaf1.

```

Leaf1(config)# vxlan 100
Leaf1(config-vxlan-100)#vxlan vniid 100
Leaf1(config-vxlan-100)#exit
Leaf1(config)# interface tengigabitethernet 0/1
Leaf1(config-if-tengigabitethernet0/1)# vxlan 100 encapsulation vlan 2
Leaf1(config-if-tengigabitethernet0/1)#exit

```

#### #Configure Leaf2.

```

Leaf2(config)# vxlan 100
Leaf2(config-vxlan-100)#vxlan vniid 100
Leaf2(config-vxlan-100)#exit
Leaf2(config)# interface tengigabitethernet 0/1
Leaf2(config-if-tengigabitethernet0/1)# vxlan 100 encapsulation vlan 2
Leaf2(config-if-tengigabitethernet0/1)#exit

```

#### #View the VXLAN information of Leaf1.

```

Leaf1#show vxlan 100 config

vxlan 100
vxlan vniid 100
exit
Leaf1#show running-config interface te0/1

interface tengigabitethernet0/1
switchport mode trunk
switchport trunk allowed vlan add 2

```

```
switchport trunk pvid vlan 10
vxlan 100 encapsulation vlan 2
exit
```

#View the VXLAN information of Leaf2.

```
Leaf2#show vxlan 100 config

vxlan 100
vxlan vniid 100
exit

Leaf2#show running-config interface te0/1

interface tengigabitethernet0/1
switchport mode trunk
switchport trunk allowed vlan add 2
switchport trunk pvid vlan 10
vxlan 100 encapsulation vlan 2
exit
```

Step 5: Configure the static VXLAN tunnel

#Configure the nve interface of Leaf1 and configure the static headend replication member corresponding to VXLAN.

```
Leaf1(config)#interface nve 1
Leaf1(config-if-nve1)#source 10.0.0.1
Leaf1(config-if-nve1)#vxlan 100 ingress-replication peer 20.0.0.1
Leaf1(config-if-nve1)#mac-address learning disable
Leaf1(config-if-nve1)#exit
```

#Configure the nve interface of Leaf2 and configure the static headend replication member corresponding to VXLAN.

```
Leaf2(config)#interface nve 1
Leaf2(config-if-nve1)#source 20.0.0.1
Leaf2(config-if-nve1)#vxlan 100 ingress-replication peer 10.0.0.1
Leaf2(config-if-nve1)#mac-address learning disable
Leaf2(config-if-nve1)#exit
```

#View the tunnel information and VXLAN session of Leaf1.

```
Leaf1#show vxlan tunnel
Reason codes: SI - Source is Invalid:
    source address is not local;
    source interface is down;
    source interface is a tunnel or management interface.
DI - Destination is Invalid:
    destination address is local;
    destination address is unreachable;
    output interface is a tunnel or management interface.
```

Number of vxlan tunnel: 1

TunnelID	Source	Destination	State
32768	10.0.0.1	20.0.0.1	up

You can see that the VXLAN tunnel on Leaf1 is successfully established and is in UP state.

```
Leaf1#show vxlan session
Number of vxlan session: 1
```

```
-----
VXLAN-ID  SessionID  TunnelID  Source      Destination  State
-----
100      32768      32768    10.0.0.1    20.0.0.1    up
```

It is indicated that the VXLAN session with the VXLAN-ID of 100 on Leaf1 is successfully bound to the tunnel with the Tunnel ID of 32768 and is in UP state.

#View the VXLAN information of Leaf2.

```
Leaf2#show vxlan tunnel
Reason codes: SI - Source is Invalid:
               source address is not local;
               source interface is down;
               source interface is a tunnel or management interface.
DI - Destination is Invalid:
               destination address is local;
               destination address is unreachable;
               output interface is a tunnel or management interface.
```

```
Number of vxlan tunnel: 1
```

```
-----
TunnelID  Source      Destination  State
-----
32768    20.0.0.1    10.0.0.1    up
```

You can see that the VXLAN tunnel on Leaf2 is successfully established and is in UP state.

```
Leaf2#show vxlan session
Number of vxlan session: 1
```

```
-----
VXLAN-ID  SessionID  TunnelID  Source      Destination  State
-----
100      32768      32768    20.0.0.1    10.0.0.1    up
```

It is indicated that the VXLAN session with the VXLAN-ID of 100 on Leaf2 is successfully bound to the tunnel with the Tunnel ID of 32768 and is in UP state.

Step 6: Check the result.

#VM1 on Server1 pings VM1 on Server2.

```
C:\Documents and Settings\ Server 1> ping 1.0.0.2

Pinging 1.0.0.2 with 32 bytes of data:

Reply from 1.0.0.2: bytes=32 time<1ms TTL=255
```

Ping statistics for 1.0.0.2:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 0ms, Maximum = 0ms, Average = 0m

It is indicated that Server1 and Server2 can be intercommunicated across the three-layer network between Leaf1 and Leaf2.

## 126.3.2 Configure BGP EVPN VXLAN for Two-layer Intercommunication

### Network Requirements

- Leaf1 and Leaf2 serve as VTEPs to create VXLAN instances.
- Leaf1 and Leaf2 create a BGP EVPN VXLAN tunnel, allowing for intercommunication between Server1 and Server2 on the same network segment.

### Network Topology

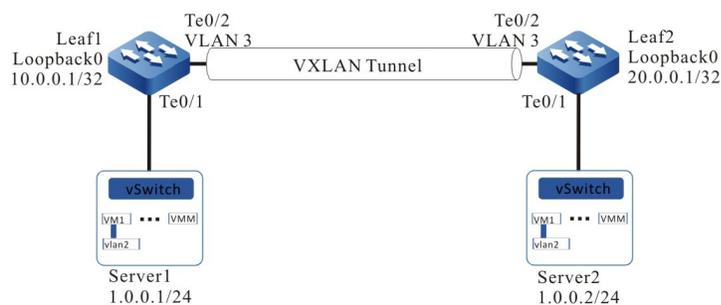


Figure 126-2 Network Topology for Configuring BGP EVPN VXLAN for Two-layer Intercommunication

### Configuration Steps

Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configure IP addresses for the ports.

#### #Configure Leaf1.

```
Leaf1(config)#interface loopback 0
Leaf1(config-if-loopback0)#ip address 10.0.0.1 255.255.255.255
Leaf1(config-if-loopback0)#exit
Leaf1(config)#interface vlan 3
Leaf1(config-if-vlan3)#ip address 2.0.0.1 255.255.255.0
Leaf1(config-if-vlan3)#exit
```

#### #Configure Leaf2.

```
Leaf2(config)#interface loopback 0
```

```
Leaf2(config-if-loopback0)#ip address 20.0.0.1 255.255.255.255
Leaf2(config-if-loopback0)#exit
Leaf2(config)#interface vlan 3
Leaf2(config-if-vlan3)#ip address 2.0.0.2 255.255.255.0
Leaf2(config-if-vlan3)#exit
```

Step 3: Configure OSPF so that the routes of Loopback between devices are reachable from each other.

#### #Configure Leaf1.

```
Leaf1#configure terminal
Leaf1(config)#router ospf 100
Leaf1(config-ospf)#network 10.0.0.1 0.0.0.0 area 0
Leaf1(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Leaf1(config-ospf)#exit
```

#### #Configure Leaf2.

```
Leaf2#configure terminal
Leaf2(config)#router ospf 100
Leaf2(config-ospf)#network 20.0.0.1 0.0.0.0 area 0
Leaf2(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Leaf2(config-ospf)#exit
```

#### #View the routing table of Leaf1.

```
Leaf1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 2.0.0.0/24 is directly connected, 00:05:40, vlan3
C 127.0.0.0/8 is directly connected, 1d:21:38:36, lo0
C 10.0.0.1/32 is directly connected, 00:06:34, loopback0
O 20.0.0.1/32 [110/2] via 2.0.0.2, 00:00:05, vlan3
```

#### #View the routing table of Leaf2.

```
Leaf2#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 2.0.0.0/24 is directly connected, 00:06:43, vlan3
C 127.0.0.0/8 is directly connected, 1w3d:03:35:57, lo0
O 10.0.0.1/32 [110/2] via 2.0.0.1, 00:02:36, vlan3
C 20.0.0.1/32 is directly connected, 00:07:07, loopback0
```

It is indicated that both Leaf1 and Leaf2 have learned the route of the loopback interface of the peer end by running the OSPF protocol.

Step 4: Configure VXLAN and associate VNID, and configure the EVPN address family so that the ports of Leaf1 and Leaf2 are added into VXLAN.

#### #Configure Leaf1.

```
Leaf1(config)# vxlan 100
```

```
Leaf1(config-vxlan-100)#vxlan vnid 100
Leaf1(config-vxlan-100)#address-family evpn
Leaf1(config-vxlan-100)#rd 100:1
Leaf1(config-vxlan-100)#route-target both 100:1
Leaf1(config-vxlan-100)#exit
Leaf1(config-vxlan-100)#exit
Leaf1(config)# interface tengigabitethernet 0/1
Leaf1(config-if-tengigabitethernet0/1)# vxlan 100 encapsulation vlan 2
Leaf1(config-if-tengigabitethernet0/1)#exit
```

#### #Configure Leaf2.

```
Leaf2(config)# vxlan 100
Leaf2(config-vxlan-100)#vxlan vnid 100
Leaf2(config-vxlan-100)#address-family evpn
Leaf2(config-vxlan-100)#rd 100:1
Leaf2(config-vxlan-100)#route-target both 100:1
Leaf2(config-vxlan-100)#exit
Leaf2(config-vxlan-100)#exit
Leaf2(config)# interface tengigabitethernet 0/1
Leaf2(config-if-tengigabitethernet0/1)# vxlan 100 encapsulation vlan 2
Leaf2(config-if-tengigabitethernet0/1)#exit
```

#### #View the VXLAN information of Leaf1.

```
Leaf1#show vxlan 100 config

vxlan 100
vxlan vnid 100
address-family evpn
rd 100:1
route-target import 100:1
route-target export 100:1
exit
exit
Leaf1#show running-config interface te0/1

interface tengigabitethernet0/1
switchport mode trunk
switchport trunk allowed vlan add 2
switchport trunk pvid vlan 10
vxlan 100 encapsulation vlan 2
exit
```

#### #View the VXLAN information of Leaf2.

```
Leaf2#show vxlan 100 config

vxlan 100
vxlan vnid 100
address-family evpn
rd 100:1
route-target import 100:1
route-target export 100:1
exit
exit
Leaf2#show running-config interface te0/1

interface tengigabitethernet0/1
switchport mode trunk
switchport trunk allowed vlan add 2
switchport trunk pvid vlan 10
vxlan 100 encapsulation vlan 2
exit
```

## Step 5: Configure BGP.

### #Configure Leaf1.

Configure to establish a direct EBGP peer in direct connection with Leaf2, and activate the advertising capability under the EVPN address family

```
Leaf1(config)#router bgp 100
Leaf1(config-bgp)#neighbor 2.0.0.2 remote-as 200
Leaf1(config-bgp)#address-family l2vpn evpn
Leaf1(config-bgp-af)#neighbor 2.0.0.2 activate
Leaf1(config-bgp-af)#exit-address-family
Leaf1(config-bgp)#exit
```

### #Configure Leaf2.

Configure to establish a direct EBGP peer in direct connection with Leaf2, and activate the advertising capability under the EVPN address family.

```
Leaf2(config)#router bgp 200
Leaf2(config-bgp)#neighbor 2.0.0.1 remote-as 100
Leaf2(config-bgp)#address-family l2vpn evpn
Leaf2(config-bgp-af)#neighbor 2.0.0.1 activate
Leaf2(config-bgp-af)#exit-address-family
Leaf2(config-bgp)#exit
```

### #Check BGP EVPN neighbors of Leaf1.

```
Leaf1#show bgp l2vpn evpn summary
BGP router identifier 10.0.0.1, local AS number 100
BGP table version is 5
1 BGP AS-PATH entries
0 BGP community entries

Neighbor    V    AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State/PfxRcd
2.0.0.2     4    200   52   50    4   0  00:42:18   0

Total number of neighbors 1
```

### #Check BGP EVPN neighbors of Leaf2.

```
Leaf2#show bgp l2vpn evpn summary
BGP router identifier 20.0.0.1, local AS number 200
BGP table version is 5
1 BGP AS-PATH entries
0 BGP community entries

Neighbor    V    AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State/PfxRcd
2.0.0.1     4    100   52   53    5   0  00:43:20   0

Total number of neighbors 1
```

It is indicated that Leaf1 and Leaf2 have successfully established BGP EVPN neighbors.

## Step 6: Create the NVE interface

#Configure the NVE interface of Leaf1 and configure the corresponding VXLAN to use the BGP protocol to dynamically establish a L2 tunnel.

```
Leaf1(config)#interface nve 1
Leaf1(config-if-nve1)#source 10.0.0.1
Leaf1(config-if-nve1)#vxlan 100 ingress-replication protocol bgp
Leaf1(config-if-nve1)#mac-address learning disable
Leaf1(config-if-nve1)#exit
```

#Configure the NVE interface of Leaf2 and configure the corresponding VXLAN to use the BGP protocol to dynamically establish a L2 tunnel.

```
Leaf2(config)#interface nve 1
Leaf2(config-if-nve1)#source 20.0.0.1
Leaf2(config-if-nve1)#vxlan 100 ingress-replication protocol bgp
Leaf2(config-if-nve1)#mac-address learning disable
Leaf2(config-if-nve1)#exit
```

#View the tunnel information and VXLAN session of Leaf1.

```
Leaf1#show vxlan tunnel
Reason codes: SI - Source is Invalid:
               source address is not local;
               source interface is down;
               source interface is a tunnel or management interface.
DI - Destination is Invalid:
               destination address is local;
               destination address is unreachable;
               output interface is a tunnel or management interface.
```

Number of vxlan tunnel: 1

TunnelID	Source	Destination	State
32768	10.0.0.1	20.0.0.1	up

```
Leaf1#show vxlan session
Number of vxlan session: 1
```

VXLAN-ID	SessionID	TunnelID	Source	Destination	State
100	32768	32768	10.0.0.1	20.0.0.1	up

#View the tunnel information of Leaf2 and the VXLAN session.

```
Leaf2#show vxlan tunnel
Reason codes: SI - Source is Invalid:
               source address is not local;
               source interface is down;
               source interface is a tunnel or management interface.
DI - Destination is Invalid:
               destination address is local;
               destination address is unreachable;
               output interface is a tunnel or management interface.
```

Number of vxlan tunnel: 1

TunnelID	Source	Destination	State
----------	--------	-------------	-------

```
32768 20.0.0.1 10.0.0.1 up
```

```
Leaf2#show vxlan session  
Number of vxlan session: 1
```

```
-----  
VXLAN-ID  SessionID  TunnelID  Source      Destination  State  
-----  
100      32768      32768     20.0.0.1    10.0.0.1    up
```

From the information described above, you can see that the tunnel is UP, and the dynamic VXLAN multicast session between Leaf1 and Leaf2 can be established normally. At this point, L2 BUM traffic can be forwarded between Leaf1 and Leaf2.

Step 7: VM1 of Server 1 and VM1 of Server 2 ping addresses absent in the same network segment, respectively, and check the VXLAN session between Leaf1 and Leaf2

#View the VXLAN session of Leaf1.

```
Leaf1#show vxlan session 20.0.0.1  
vxlan session 32768  
state: up  
source IP: 10.0.0.1  
destination IP: 20.0.0.1  
source mac: 0001.7a00.5278  
destination mac: 0001.7a21.81e7  
interface: vlan3  
switchport: tengigabitethernet0/2  
vxlan list: 100  
vxlan unicast list: 100  
vxlan multicast list: 100
```

#View the VXLAN session of Leaf2.

```
Leaf2#show vxlan session 10.0.0.1  
vxlan session 32768  
state: up  
source IP: 20.0.0.1  
destination IP: 10.0.0.1  
source mac: 0001.7a21.81e7  
destination mac: 0001.7a00.5278  
interface: vlan3  
switchport: tengigabitethernet0/2  
vxlan list: 100  
vxlan unicast list: 100  
vxlan multicast list: 100
```

It is indicated that all dynamic unicast sessions have been established, with L2 unicast traffic available for forwarding

Step 8: Check the result.

#Ping VM1 of Server2 on VM1 of Server1.

```
C:\Documents and Settings\ Server 1> ping 1.0.0.2
```

Pinging 1.0.0.2 with 32 bytes of data:

```
Reply from 1.0.0.2: bytes=32 time<1ms TTL=255
```

Ping statistics for 1.0.0.2:

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0m
```

It is indicated that Server1 and Server2 can be intercommunicated across the three-layer network between Leaf1 and Leaf2.

---

## Note

- BGP EVPN supports IBGP and EBGP.
  - After BGP enables the EVPN VXLAN capability, BGP neighbors will be automatically reestablished.
- 

### 126.3.3 Configure Static Centralized VXLAN Gateway

#### Network Requirements

- Create VXLAN instances on Leaf1, Spine1, and Leaf2, respectively.
- Leaf1, Spine1, and Leaf2 establish a static VXLAN tunnel via the loopback interface, which tunnel acts as a centralized VXLAN gateway on Spine1 for intercommunication between Server1 and Server3 on the same network segment and between Server2 and Server3 on different network segments.

#### Network Topology

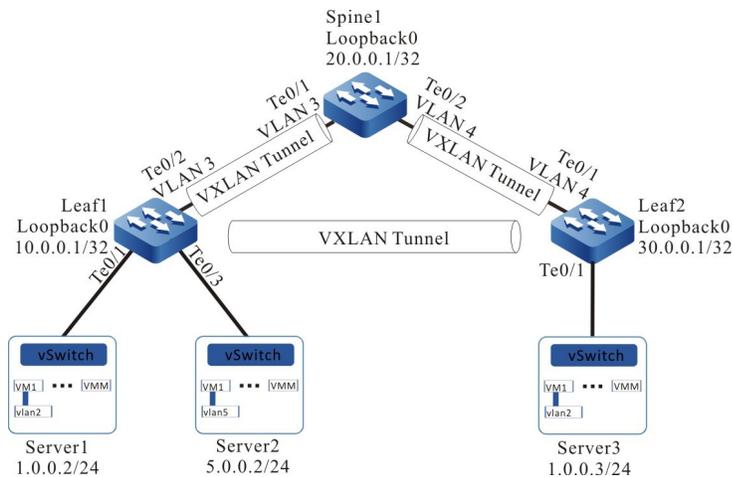


Figure 126-3 Network Topology for Configuring Static Centralized VXLAN Gateway

### Configuration Steps

Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configure IP addresses for the ports.

#### #Configure Leaf1.

```
Leaf1(config)#interface loopback 0
Leaf1(config-if-loopback0)#ip address 10.0.0.1 255.255.255.255
Leaf1(config-if-loopback0)#exit
Leaf1(config)#interface vlan 3
Leaf1(config-if-vlan3)#ip address 2.0.0.1 255.255.255.0
Leaf1(config-if-vlan3)#exit
```

#### #Configure Spine1.

```
Spine1(config)#interface loopback 0
Spine1(config-if-loopback0)#ip address 20.0.0.1 255.255.255.255
Spine1(config-if-loopback0)#exit
Spine1(config)#interface vlan 3
Spine1(config-if-vlan3)#ip address 2.0.0.2 255.255.255.0
Spine1(config-if-vlan3)#exit
Spine1(config)#interface vlan 4
Spine1(config-if-vlan4)#ip address 3.0.0.1 255.255.255.0
Spine1(config-if-vlan4)#exit
```

#### #Configure Leaf2.

```
Leaf2(config)#interface loopback 0
Leaf2(config-if-loopback0)#ip address 30.0.0.1 255.255.255.255
Leaf2(config-if-loopback0)#exit
Leaf2(config)#interface vlan 4
Leaf2(config-if-vlan4)#ip address 3.0.0.2 255.255.255.0
Leaf2(config-if-vlan4)#exit
```

Step 3: Configure OSPF so that the routes of Loopback between devices are reachable from each other.

#### #Configure Leaf1.

```
Leaf1#configure terminal
Leaf1(config)#router ospf 100
Leaf1(config-ospf)#network 10.0.0.1 0.0.0.0 area 0
Leaf1(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Leaf1(config-ospf)#exit
```

#### #Configure Spine1.

```
Spine1#configure terminal
Spine1(config)#router ospf 100
Spine1(config-ospf)#network 20.0.0.1 0.0.0.0 area 0
Spine1(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Spine1(config-ospf)#network 3.0.0.0 0.0.0.255 area 0
Spine1(config-ospf)#exit
```

#### #Configure Leaf2.

```
Leaf2#configure terminal
Leaf2(config)#router ospf 100
Leaf2(config-ospf)#network 30.0.0.1 0.0.0.0 area 0
Leaf2(config-ospf)#network 3.0.0.0 0.0.0.255 area 0
Leaf2(config-ospf)#exit
```

#### #View the routing table of Leaf1.

```
Leaf1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 2.0.0.0/24 is directly connected, 00:28:27, vlan3
O 3.0.0.0/24 [110/2] via 2.0.0.2, 00:00:05, vlan3
C 127.0.0.0/8 is directly connected, 2d:23:06:31, lo0
C 10.0.0.1/32 is directly connected, 1d:01:34:29, loopback0
O 20.0.0.1/32 [110/2] via 2.0.0.2, 00:00:05, vlan3
O 30.0.0.1/32 [110/3] via 2.0.0.2, 00:00:05, vlan3
```

#### #View the routing table of Spine1.

```
Spine1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 2.0.0.0/24 is directly connected, 07:04:46, vlan3
C 3.0.0.0/24 is directly connected, 00:23:50, vlan4
C 127.0.0.0/8 is directly connected, 1w4d:05:02:08, lo0
O 10.0.0.1/32 [110/2] via 2.0.0.1, 00:00:57, vlan3
C 20.0.0.1/32 is directly connected, 1d:01:33:17, loopback0
O 30.0.0.1/32 [110/2] via 3.0.0.2, 00:01:33, vlan4
```

#### #View the routing table of Leaf2.

```
Leaf2#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

- O 2.0.0.0/24 [110/2] via 3.0.0.1, 00:02:43, vlan4
- C 3.0.0.0/24 is directly connected, 00:22:14, vlan4
- C 30.0.0.0/24 is directly connected, 00:23:24, loopback0
- C 127.0.0.0/8 is directly connected, 4d:00:16:59, lo0
- O 10.0.0.1/32 [110/3] via 3.0.0.1, 00:02:07, vlan4
- O 20.0.0.1/32 [110/2] via 3.0.0.1, 00:02:43, vlan4

You can see that Leaf1, Spine1 and Leaf2 all have learned the route of the loopback interface of the peer end by running the OSPF protocol.

Step 4: Configure VXLAN and associate VNID so that the ports of Leaf1 and Spine1 are added into VXLAN.

#### #Configure Leaf1.

```
Leaf1(config)#vxlان 100
Leaf1(config-vxlan-100)#vxlan vnid 100
Leaf1(config-vxlan-100)#exit
Leaf1(config)# interface tengigabitethernet 0/1
Leaf1(config-if-tengigabitethernet0/1)# vxlan 100 encapsulation vlan 2
Leaf1(config-if-tengigabitethernet0/1)#exit

Leaf1(config)#vxlان 200
Leaf1(config-vxlan-200)#vxlan vnid 200
Leaf1(config-vxlan-200)#exit
Leaf1(config)# interface tengigabitethernet 0/3
Leaf1(config-if-tengigabitethernet0/3)# vxlan 200 encapsulation vlan 5
Leaf1(config-if-tengigabitethernet0/3)#exit
```

#### #Configure Spine1.

```
Spine1(config)#vxlان 100
Spine1(config-vxlan-100)#vxlan vnid 100
Spine1(config-vxlan-100)#exit
Spine1(config)# vxlan 200
Spine1(config-vxlan-200)#vxlan vnid 200
Spine1(config-vxlan-200)#exit
```

#### #Configure Leaf2.

```
Leaf2(config)#vxlان 100
Leaf2(config-vxlan-100)#vxlan vnid 100
Leaf2(config-vxlan-100)#exit
Leaf2(config)# interface tengigabitethernet 0/1
Leaf2(config-if-tengigabitethernet0/1)# vxlan 100 encapsulation vlan 2
Leaf2(config-if-tengigabitethernet0/1)#exit
```

#### #View the VXLAN information of Leaf1.

```
Leaf1#show vxlan config

vxlan 100
vxlan vnid 100
exit
```

```
vxlan 200
vxlan vnid 200
exit
```

```
Leaf1#show running-config interface te0/1
```

```
interface tengigabitethernet0/1
switchport mode trunk
switchport trunk allowed vlan add 2
switchport trunk pvid vlan 10
vxlan 100 encapsulation vlan 2
exit
```

```
Leaf1#show running-config interface te0/3
```

```
interface tengigabitethernet0/3
switchport mode trunk
switchport trunk allowed vlan add 5
switchport trunk pvid vlan 10
vxlan 100 encapsulation vlan 5
exit
```

### #View the VXLAN information of Spine1.

```
Spine1#show vxlan config
```

```
vxlan 100
vxlan vnid 100
exit
vxlan 200
vxlan vnid 200
exit
```

### #View the VXLAN information of Leaf2.

```
Leaf2#show vxlan config
```

```
vxlan 100
vxlan vnid 100
exit
```

```
Leaf1#show running-config interface te0/1
```

```
interface tengigabitethernet0/1
switchport mode trunk
switchport trunk allowed vlan add 2
switchport trunk pvid vlan 10
vxlan 100 encapsulation vlan 2
exit
```

### Step 5: Configure the static VXLAN tunnel

### #Configure the nve interface of Leaf1 and configure the static headend replication member corresponding to VXLAN.

```
Leaf1(config)#interface nve 1
Leaf1(config-if-nve1)#source 10.0.0.1
Leaf1(config-if-nve1)#vxlan 100 ingress-replication peer 20.0.0.1
Leaf1(config-if-nve1)#vxlan 100 ingress-replication peer 30.0.0.1
Leaf1(config-if-nve1)#vxlan 200 ingress-replication peer 20.0.0.1
Leaf1(config-if-nve1)#mac-address learning disable
Leaf1(config-if-nve1)#exit
```

#Configure the nve interface of Leaf1 and configure the static headend replication member corresponding to VXLAN.

```
Spine1(config)#interface nve 1
Spine1(config-if-nve1)#source 20.0.0.1
Spine1(config-if-nve1)#vxlan 100 ingress-replication peer 10.0.0.1
Spine1(config-if-nve1)#vxlan 100 ingress-replication peer 30.0.0.1
Spine1(config-if-nve1)#vxlan 200 ingress-replication peer 10.0.0.1
Spine1 (config-if-nve1)#mac-address learning disable
Spine1(config-if-nve1)#exit
```

#Configure the nve interface of Leaf2 and configure the static headend replication member corresponding to VXLAN.

```
Leaf2(config)#interface nve 1
Leaf2(config-if-nve1)#source 30.0.0.1
Leaf2(config-if-nve1)#vxlan 100 ingress-replication peer 10.0.0.1
Leaf2(config-if-nve1)#vxlan 100 ingress-replication peer 20.0.0.1
Leaf2(config-if-nve1)#mac-address learning disable
Leaf2(config-if-nve1)#exit
```

#View the tunnel information and VXLAN session of Leaf1.

```
Leaf1#show vxlan tunnel
Reason codes: SI - Source is Invalid:
               source address is not local;
               source interface is down;
               source interface is a tunnel or management interface.
DI - Destination is Invalid:
               destination address is local;
               destination address is unreachable;
               output interface is a tunnel or management interface.
```

Number of vxlan tunnel: 2

TunnelID	Source	Destination	State
32768	10.0.0.1	20.0.0.1	up
32769	10.0.0.1	30.0.0.1	up

```
Leaf1#show vxlan session
Number of vxlan session: 3
```

VXLAN-ID	SessionID	TunnelID	Source	Destination	State
100	32768	32768	10.0.0.1	20.0.0.1	up
100	32769	32769	10.0.0.1	30.0.0.1	up
200	32768	32768	10.0.0.1	20.0.0.1	up

It is indicated that the VXLAN sessions with VXLAN-IDs of 100 and 200 share the same tunnel with the Tunnel ID of 32768.

#View the tunnel information and VXLAN session of Spine1.

```
Spine1#show vxlan tunnel
Reason codes: SI - Source is Invalid:
               source address is not local;
               source interface is down;
               source interface is a tunnel or management interface.
DI - Destination is Invalid:
               destination address is local;
```

destination address is unreachable;  
output interface is a tunnel or management interface.

Number of vxlan tunnel: 2

TunnelID	Source	Destination	State
32768	20.0.0.1	10.0.0.1	up
32769	20.0.0.1	30.0.0.1	up

Spine1#show vxlan session  
Number of vxlan session: 3

VXLAN-ID	SessionID	TunnelID	Source	Destination	State
100	32768	32768	20.0.0.1	10.0.0.1	up
100	32769	32769	20.0.0.1	30.0.0.1	up
200	32768	32768	20.0.0.1	10.0.0.1	up

### #View the tunnel information and VXLAN session of Leaf2.

Leaf2#show vxlan tunnel

Reason codes: SI - Source is Invalid:  
source address is not local;  
source interface is down;  
source interface is a tunnel or management interface.  
DI - Destination is Invalid:  
destination address is local;  
destination address is unreachable;  
output interface is a tunnel or management interface.

Number of vxlan tunnel: 2

TunnelID	Source	Destination	State
32768	30.0.0.1	10.0.0.1	up
32769	30.0.0.1	20.0.0.1	up

Leaf2#show vxlan session  
Number of vxlan session: 2

VXLAN-ID	SessionID	TunnelID	Source	Destination	State
100	32768	32768	30.0.0.1	10.0.0.1	up
100	32769	32769	30.0.0.1	20.0.0.1	up

The information described above indicates that the tunnel is UP, the VXLAN session state is active and VXLAN is correctly associated.

### Step 6: Configure the VXLAN L3 gateway on Spine1.

```
Spine1(config)#interface vxlan 100
Spine1(config-if-vxlan100)#ip address 1.0.0.1 24
Spine1(config-if-vxlan100)#exit
Spine1(config)#int vxlan 200
Spine1(config-if-vxlan200)#ip address 5.0.0.1 24
Spine1(config-if-vxlan200)#exit
```

### #View the interface VXLAN interface and routing table of Spine1.

Spine1#show interface vxlan 100  
vxlan100:

```

line protocol is up
Flags: (0xc008063) BROADCAST MULTICAST ARP RUNNING
Type: ETHERNET_CSMACD
Internet address: 1.0.0.1/24
Broadcast address: 1.0.0.255
Metric: 0, MTU: 1500, BW: 100000 Kbps, DLY: 100 usec, VRF: global
Reliability 255/255, Txload 1/255, Rxload 1/255
Ethernet address is 0001.7a21.81e7
5 minutes input rate 0 bits/sec, 0 packets/sec
5 minutes output rate 0 bits/sec, 0 packets/sec
1 packets received; 2 packets sent
1 multicast packets received
2 multicast packets sent
0 input errors; 0 output errors
0 collisions; 0 dropped
Unknown protocol 0

```

```
Spine1#show interface vxlan 200
```

```
vxlan200:
```

```

line protocol is up
Flags: (0xc008063) BROADCAST MULTICAST ARP RUNNING
Type: ETHERNET_CSMACD
Internet address: 5.0.0.1/24
Broadcast address: 5.0.0.255
Metric: 0, MTU: 1500, BW: 100000 Kbps, DLY: 100 usec, VRF: global
Reliability 255/255, Txload 1/255, Rxload 1/255
Ethernet address is 0001.7a21.81e7
5 minutes input rate 0 bits/sec, 0 packets/sec
5 minutes output rate 0 bits/sec, 0 packets/sec
0 packets received; 2 packets sent
0 multicast packets received
2 multicast packets sent
0 input errors; 0 output errors
0 collisions; 0 dropped
Unknown protocol 0

```

```
Spine1#show ip route
```

```
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
```

```
U - Per-user Static route
```

```
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```

C 1.0.0.0/24 is directly connected, 00:02:08, vxlan100
C 2.0.0.0/24 is directly connected, 07:51:05, vlan3
C 3.0.0.0/24 is directly connected, 01:10:08, vlan4
C 5.0.0.0/24 is directly connected, 00:01:58, vxlan200
C 127.0.0.0/8 is directly connected, 1w4d:05:48:26, lo0
O 10.0.0.1/32 [110/2] via 2.0.0.1, 00:47:15, vlan3
C 20.0.0.1/32 is directly connected, 1d:02:19:36, loopback0
O 30.0.0.1/32 [110/2] via 3.0.0.2, 00:47:51, vlan4

```

Step 7: Check the result.

#Configure the gateways on Server1, Server2 and Server3.

#Ping Server1 on Server3.

```
C:\Documents and Settings\ Server 3> ping 1.0.0.2
```

```
Pinging 1.0.0.2 with 32 bytes of data:
```

```
Reply from 1.0.0.2: bytes=32 time<1ms TTL=255
```

```
Reply from 1.0.0.2: bytes=32 time<1ms TTL=255
```

```
Reply from 1.0.0.2: bytes=32 time<1ms TTL=255
Reply from 1.0.0.2: bytes=32 time<1ms TTL=255
```

```
Ping statistics for 1.0.0.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0m
```

You can see that Server1 and Server3 can be intercommunicated across the three-layer network between Leaf1, Spine1 and Leaf2.

#Ping Server2 on Server3.

```
C:\Documents and Settings\ Server 3> ping 5.0.0.2
```

```
Pinging 5.0.0.2 with 32 bytes of data:
```

```
Reply from 5.0.0.2: bytes=32 time<1ms TTL=255
```

```
Ping statistics for 5.0.0.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0m
```

You can see that Server2 and Server3 can be intercommunicated across the three-layer network between Leaf1, Spine1 and Leaf2.

## 126.3.4 Configure BGP EVPN VXLAN Centralized Active-Active Gateway

### Network Requirements

- Create VXLAN instances on Leaf1, Leaf2, Spine1, and Spine2, respectively.
- Leaf1, Leaf2, Spine1, and Spine2 use MP-IBGP to get through the EVPN route, create the IBGP EVPN VXLAN tunnel, and create the VXLAN centralized gateway on Spine1 and Spine2, allowing for intercommunication between VM1 of Server1 and VM1 of Server2 on different network segments.

### Network Topology

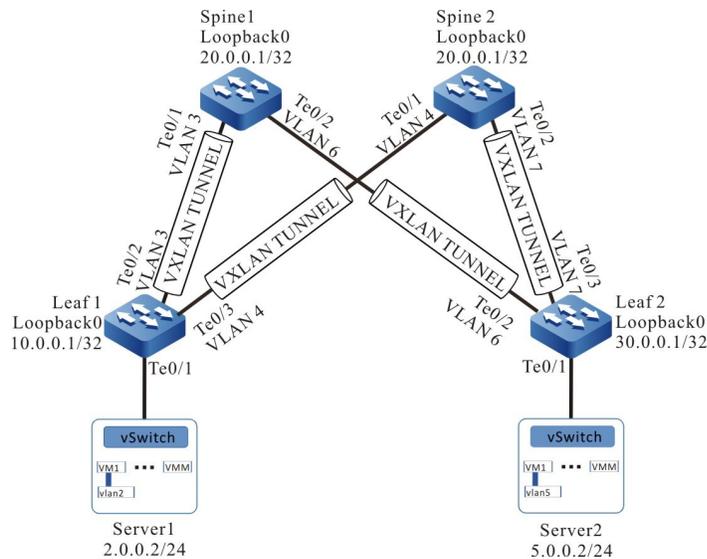


Figure 126-4 Network Topology for Configuring BGP EVPN VXLAN Centralized Active-Active Gateway

### Configuration Steps

Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configure IP addresses for the ports.

#### #Configure Leaf1.

```
Leaf1(config)#interface loopback 0
Leaf1(config-if-loopback0)#ip address 10.0.0.1 255.255.255.255
Leaf1(config-if-loopback0)#exit
Leaf1(config)#interface vlan 3
Leaf1(config-if-vlan3)#ip address 3.0.0.1 255.255.255.0
Leaf1(config-if-vlan3)#exit
Leaf1(config)#interface vlan 4
Leaf1(config-if-vlan4)#ip address 4.0.0.1 255.255.255.0
Leaf1(config-if-vlan4)#exit
```

#### #Configure Leaf2.

```
Leaf2(config)#interface loopback 0
Leaf2(config-if-loopback0)#ip address 30.0.0.1 255.255.255.255
Leaf2(config-if-loopback0)#exit
Leaf2(config)#interface vlan 6
Leaf2(config-if-vlan6)#ip address 6.0.0.2 255.255.255.0
Leaf2(config-if-vlan6)#exit
Leaf2(config)#interface vlan 7
Leaf2(config-if-vlan7)#ip address 7.0.0.2 255.255.255.0
Leaf2(config-if-vlan7)#exit
```

#### #Configure Spine1.

```
Spine1(config)#interface loopback 0
Spine1(config-if-loopback0)#ip address 20.0.0.1 255.255.255.255
```

```

Spine1(config-if-loopback0)#exit
Spine1(config)#interface loopback 1
Spine1(config-if-loopback1)#ip address 20.0.1.1 255.255.255.255
Spine1(config-if-loopback1)#exit
Spine1(config)#interface vlan 3
Spine1(config-if-vlan3)#ip address 3.0.0.2 255.255.255.0
Spine1(config-if-vlan3)#exit
Spine1(config)#interface vlan 6
Spine1(config-if-vlan6)#ip address 6.0.0.2 255.255.255.0
Spine1(config-if-vlan6)#exit

```

### #Configure Spine2.

```

Spine2(config)#interface loopback 0
Spine2(config-if-loopback0)#ip address 20.0.0.1 255.255.255.255
Spine2(config-if-loopback0)#exit
Spine2(config)#interface loopback 1
Spine2(config-if-loopback1)#ip address 20.0.2.1 255.255.255.255
Spine2(config-if-loopback1)#exit
Spine2(config)#interface vlan 4
Spine2(config-if-vlan4)#ip address 4.0.0.2 255.255.255.0
Spine2(config-if-vlan4)#exit
Spine2(config)#interface vlan 7
Spine2(config-if-vlan7)#ip address 7.0.0.2 255.255.255.0
Spine2(config-if-vlan7)#exit

```

Step 3: Configure OSPF so that the routes of Loopback between devices are reachable from each other.

### #Configure Leaf1.

```

Leaf1#configure terminal
Leaf1(config)#router ospf 100
Leaf1(config-ospf)#network 10.0.0.1 0.0.0.0 area 0
Leaf1(config-ospf)#network 3.0.0.0 0.0.0.255 area 0
Leaf1(config-ospf)#network 4.0.0.0 0.0.0.255 area 0
Leaf1(config-ospf)#exit

```

### #Configure Leaf2, Spine1 and Spine2 with reference to Leaf1

### #View the routing table of Leaf1.

```

Leaf1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 3.0.0.0/24 is directly connected, 02:47:02, vlan3
C 4.0.0.0/24 is directly connected, 02:46:43, vlan4
O 6.0.0.0/24 [110/2] via 3.0.0.2, 02:32:02, vlan3
O 7.0.0.0/24 [110/2] via 4.0.0.2, 02:31:22, vlan4
C 127.0.0.0/8 is directly connected, 21:16:50, lo0
C 10.0.0.1/32 is directly connected, 02:51:55, loopback0
O 20.0.0.1/32 [110/2] via 3.0.0.2, 02:32:02, vlan3
   [110/2] via 4.0.0.2, 02:31:32, vlan4
O 20.0.1.1/32 [110/2] via 3.0.0.2, 01:51:02, vlan3
O 20.0.2.1/32 [110/2] via 4.0.0.2, 01:53:11, vlan4
O 30.0.0.1/32 [110/3] via 3.0.0.2, 02:32:02, vlan3
   [110/3] via 4.0.0.2, 02:31:22, vlan4

```

You can see that Leaf1 has learned the route of the loopback interface of the peer end by running the OSPF protocol.

Step 4: Configure VXLAN and associate VNID, and configure the EVPN address family so that the ports of Leaf1 and Leaf2 are added into VXLAN.

#### #Configure Leaf1.

```
Leaf1(config)# vxlan 100
Leaf1(config-vxlan-100)#vxlan vniid 100
Leaf1(config-vxlan-100)#address-family evpn
Leaf1(config-vxlan-evpn)#rd 100:1
Leaf1(config-vxlan-evpn)#route-target both 100:1
Leaf1(config-vxlan-evpn)#exit
Leaf1(config-vxlan-100)#exit
Leaf1(config)# interface tengigabitethernet 0/1
Leaf1(config-if-tengigabitethernet0/1)# vxlan 100 encapsulation vlan 2
Leaf1(config-if-tengigabitethernet0/1)#exit
```

#### #Configure Leaf2.

```
Leaf2(config)# vxlan 200
Leaf2(config-vxlan-200)# vxlan vniid 200
Leaf2(config-vxlan-200)#address-family evpn
Leaf2(config-vxlan-evpn)#rd 200:1
Leaf2(config-vxlan-evpn)#route-target both 200:1
Leaf2(config-vxlan-evpn)#exit
Leaf2(config-vxlan-200)#exit
Leaf2(config)# interface tengigabitethernet 0/1
Leaf2(config-if-tengigabitethernet0/1)# vxlan 200 encapsulation vlan 5
Leaf2(config-if-tengigabitethernet0/1)#exit
```

#### #Configure Spine1.

```
Spine1(config)# vxlan 100
Spine1(config-vxlan-100)#vxlan vniid 100
Spine1(config-vxlan-100)#address-family evpn
Spine1(config-vxlan-evpn)#rd 100:1
Spine1(config-vxlan-evpn)#route-target both 100:1
Spine1(config-vxlan-evpn)#exit
Spine1(config-vxlan-100)#exit
Spine1(config)# vxlan 200
Spine1(config-vxlan-200)# vxlan vniid 200
Spine1(config-vxlan-200)#address-family evpn
Spine1(config-vxlan-evpn)#rd 200:1
Spine1(config-vxlan-evpn)#route-target both 200:1
Spine1(config-vxlan-evpn)#exit
Spine1(config-vxlan-200)#exit
```

#### #Configure Spine2.

```
Spine2(config)# vxlan 100
Spine2(config-vxlan-100)#vxlan vniid 100
Spine2(config-vxlan-100)#address-family evpn
Spine2(config-vxlan-evpn)#rd 100:1
Spine2(config-vxlan-evpn)#route-target both 100:1
Spine2(config-vxlan-evpn)#exit
Spine2(config-vxlan-100)#exit
Spine2(config)# vxlan 200
Spine2(config-vxlan-200)# vxlan vniid 200
```

```
Spine2(config-vxlan-200)#address-family evpn
Spine2(config-vxlan-200)#rd 200:1
Spine2(config-vxlan-200)#route-target both 200:1
Spine2(config-vxlan-200)#exit
Spine2(config-vxlan-200)#exit
```

### #View the VXLAN information of Leaf1.

```
Leaf1#show vxlan config

vxlan 100
vxlan vniid 100
address-family evpn
rd 100:1
route-target import 100:1
route-target export 100:1
exit
exit
Leaf1#show running-config interface te0/1

interface tengigabitethernet0/1
switchport mode trunk
switchport trunk allowed vlan add 2
switchport trunk pvid vlan 10
vxlan 100 encapsulation vlan 2
exit
```

### #View the VXLAN information of Leaf2.

```
Leaf2#show vxlan config

vxlan 200
vxlan vniid 200
address-family evpn
rd 200:1
route-target import 200:1
route-target export 200:1
exit
exit
Leaf2#show running-config interface te0/1

interface tengigabitethernet0/1
switchport mode trunk
switchport trunk allowed vlan add 5
switchport trunk pvid vlan 10
vxlan 200 encapsulation vlan 5
exit
```

### #View the VXLAN information of Spine1.

```
Spine1#show vxlan config

vxlan 100
vxlan vniid 100
address-family evpn
rd 100:1
route-target import 100:1
route-target export 100:1
exit
exit
```

```
vxlan 200
vxlan vniid 200
address-family evpn
rd 200:1
route-target import 200:1
route-target export 200:1
exit
exit
```

#### #View the VXLAN information of Spine2.

```
Spine2#show vxlan config

vxlan 100
vxlan vniid 100
address-family evpn
rd 100:1
route-target import 100:1
route-target export 100:1
exit
exit
vxlan 200
vxlan vniid 200
address-family evpn
rd 200:1
route-target import 200:1
route-target export 200:1
exit
exit
```

#### Step 5: Configure BGP.

##### #Configure Leaf1.

Configure to establish the IBGP peers to Spine1 and Spine2, and activate the advertising capability under the EVPN address family.

```
Leaf1(config)#router bgp 100
Leaf1(config-bgp)#neighbor 20.0.1.1 remote-as 100
Leaf1(config-bgp)#neighbor 20.0.1.1 update-source loopback0
Leaf1(config-bgp)#neighbor 20.0.2.1 remote-as 100
Leaf1(config-bgp)#neighbor 20.0.1.1 update-source loopback0
Leaf1(config-bgp)#address-family l2vpn evpn
Leaf1(config-bgp-af)#neighbor 20.0.1.1 activate
Leaf1(config-bgp-af)#neighbor 20.0.2.1 activate
Leaf1(config-bgp-af)#exit-address-family
Leaf1(config-bgp)#exit
```

##### #Configure Spine1.

Configure to establish the IBGP peers to Leaf1 and Leaf2, and activate the advertising capability and reflector client under the EVPN address family.

```
Spine1(config)#router bgp 100
Spine1(config-bgp)#neighbor 10.0.0.1 remote-as 100
Spine1(config-bgp)#neighbor 10.0.0.1 update-source loopback1
Spine1(config-bgp)#neighbor 30.0.0.1 remote-as 100
Spine1(config-bgp)#neighbor 30.0.0.1 update-source loopback1
Spine1(config-bgp)#address-family l2vpn evpn
```

```

Spine1(config-bgp-af)#neighbor 10.0.0.1 activate
Spine1(config-bgp-af)#neighbor 10.0.0.1 route-reflector-client
Spine1(config-bgp-af)#neighbor 30.0.0.1 activate
Spine1(config-bgp-af)#neighbor 30.0.0.1 route-reflector-client
Spine1(config-bgp-af)#exit-address-family
Spine1(config-bgp)#exit

```

#Configure Leaf2, configure to establish the IBGP peers to Spine1 and Spine2, and activate the advertising capability under the EVPN address family. For the configurations, refer to the configuration of Leaf1.

#Configure Spine2, configure to establish the IBGP peers to Leaf1 and Leaf2, and activate the advertising capability and reflector client under the EVPN address family. For the configurations, refer to the configuration of Spine1.

#Check BGP EVPN neighbors of Leaf1.

```

Leaf1#show bgp l2vpn evpn summary
BGP router identifier 10.0.0.1, local AS number 100
BGP table version is 1
1 BGP AS-PATH entries
0 BGP community entries

Neighbor    V    AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State/PfxRcd
20.0.1.1    4    100   12   12    1  0  0 00:09:05    0
20.0.2.1    4    100    2    2    1  0  0 00:00:21    0

Total number of neighbors 2

```

#Check BGP EVPN neighbors of Spine1.

```

Spine1#show bgp l2vpn evpn summary
BGP router identifier 20.0.1.1, local AS number 100
BGP table version is 1
1 BGP AS-PATH entries
0 BGP community entries

Neighbor    V    AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State/PfxRcd
10.0.0.1    4    100   12   12    1  0  0 00:09:17    0
30.0.0.1    4    100    3    3    1  0  0 00:01:14    0

Total number of neighbors 2

```

Step 6: Configure the NVE interface and VM to trigger ARP learning.

#Configure the NVE interface of Leaf1 and configure the corresponding VXLAN to use the BGP protocol to dynamically establish a VXLAN tunnel.

```

Leaf1(config)#interface nve 1
Leaf1(config-if-nve1)#source 10.0.0.1
Leaf1(config-if-nve1)#vxlan 100 ingress-replication protocol bgp
Leaf1(config-if-nve1)#mac-address learning disable
Leaf1(config-if-nve1)#exit

```

#Configure the NVE interface of Leaf2 and configure the corresponding VXLAN to use the BGP protocol to dynamically establish a VXLAN tunnel.

```
Leaf2(config)#interface nve 1
Leaf2(config-if-nve1)#source 30.0.0.1
Leaf2(config-if-nve1)#vxlan 200 ingress-replication protocol bgp
Leaf2(config-if-nve1)#mac-address learning disable
Leaf2(config-if-nve1)#exit
```

#Configure the NVE interface of Spine1 and configure the corresponding VXLAN to use the BGP protocol to dynamically establish a VXLAN tunnel.

```
Spine1(config)#interface nve 1
Spine1(config-if-nve1)#source 20.0.0.1
Spine1(config-if-nve1)#vxlan 100,200 ingress-replication protocol bgp
Spine1(config-if-nve1)#mac-address learning disable
Spine1(config-if-nve1)#exit
```

#Configure the NVE interface of Spine2 and configure the corresponding VXLAN to use the BGP protocol to dynamically establish a VXLAN tunnel.

```
Spine2(config)#interface nve 1
Spine2(config-if-nve1)#source 20.0.0.1
Spine2(config-if-nve1)#vxlan 100,200 ingress-replication protocol bgp
Spine2(config-if-nve1)#mac-address learning disable
Spine2(config-if-nve1)#exit
```

#VM1 on Server1 and VM1 on Server2 ping the addresses absent on the same network segment, respectively.

## Step 7: Create the VXLAN L3 gateways on Spine1 and Spine2

#Create the VXLAN L3 gateway on Spine1

```
Spine1(config)#interface vxlan 100
Spine1(config-if-vxlan100)#ip address 2.0.0.1 24
Spine1(config-if-vxlan100)#mac-address 0000.5e00.0101
Spine1(config-if-vxlan100)#exit
Spine1(config)#int vxlan 200
Spine1(config-if-vxlan200)#ip address 5.0.0.1 24
Spine1(config-if-vxlan200)#mac-address 0000.5e00.0102
Spine1(config-if-vxlan200)#exit
```

#Create the VXLAN L3 gateway on Spine2

```
Spine2(config)#interface vxlan 100
Spine2(config-if-vxlan100)#ip address 2.0.0.1 24
Spine2(config-if-vxlan100)#mac-address 0000.5e00.0101
Spine2(config-if-vxlan100)#exit
Spine2(config)#int vxlan 200
Spine2(config-if-vxlan200)#ip address 5.0.0.1 24
Spine2(config-if-vxlan200)#mac-address 0000.5e00.0102
Spine2(config-if-vxlan200)#exit
```

#View the interface VXLAN interface and routing table of Spine1.

```
Spine1#show interface vxlan 100
vxlan100:
```

```

line protocol is up
Flags: (0xc008063) BROADCAST MULTICAST ARP RUNNING
Type: ETHERNET_CSMACD
Internet address: 2.0.0.1/24
Broadcast address: 2.0.0.255
Metric: 0, MTU: 1500, BW: 100000 Kbps, DLY: 100 usec, VRF: global
Reliability 255/255, Txload 1/255, Rxload 1/255
Ethernet address is 0000.5e00.0101
5 minutes input rate 0 bits/sec, 0 packets/sec
5 minutes output rate 0 bits/sec, 0 packets/sec
0 packets received; 1 packets sent
0 multicast packets received
1 multicast packets sent
0 input errors; 0 output errors
0 collisions; 0 dropped
Unknown protocol 0

```

```

Spine1#show interface vxlan 200
vxlan200:

```

```

line protocol is up
Flags: (0xc008063) BROADCAST MULTICAST ARP RUNNING
Type: ETHERNET_CSMACD
Internet address: 5.0.0.1/24
Broadcast address: 5.0.0.255
Metric: 0, MTU: 1500, BW: 100000 Kbps, DLY: 100 usec, VRF: global
Reliability 255/255, Txload 1/255, Rxload 1/255
Ethernet address is 0000.5e00.0102
5 minutes input rate 0 bits/sec, 0 packets/sec
5 minutes output rate 0 bits/sec, 0 packets/sec
0 packets received; 1 packets sent
0 multicast packets received
1 multicast packets sent
0 input errors; 0 output errors
0 collisions; 0 dropped
Unknown protocol 0

```

```

Spine1#show ip route

```

```

Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS

```

```

U - Per-user Static route

```

```

O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

```

```

C 2.0.0.0/24 is directly connected, 00:31:28, vxlan100
C 3.0.0.0/24 is directly connected, 04:05:05, vlan3
O 4.0.0.0/24 [110/2] via 3.0.0.1, 03:47:46, vlan3
C 5.0.0.0/24 is directly connected, 00:04:32, vxlan200
C 6.0.0.0/24 is directly connected, 04:04:53, vlan6
O 7.0.0.0/24 [110/2] via 6.0.0.1, 03:47:35, vlan6
C 127.0.0.0/8 is directly connected, 3d:19:46:04, lo0
O 10.0.0.1/32 [110/2] via 3.0.0.1, 03:52:27, vlan3
C 20.0.0.1/32 is directly connected, 04:05:42, loopback0
C 20.0.1.1/32 is directly connected, 03:07:49, loopback1
O 20.0.2.1/32 [110/3] via 3.0.0.1, 03:09:24, vlan3
[110/3] via 6.0.0.1, 03:09:24, vlan6
O 30.0.0.1/32 [110/2] via 6.0.0.1, 03:52:27, vlan6

```

## #View the interface VXLAN interface and routing table of Spine2.

```

Spine2#show interface vxlan 100

```

```

vxlan100:

```

```

line protocol is up
Flags: (0xc008063) BROADCAST MULTICAST ARP RUNNING
Type: ETHERNET_CSMACD
Internet address: 2.0.0.1/24
Broadcast address: 2.0.0.255
Metric: 0, MTU: 1500, BW: 100000 Kbps, DLY: 100 usec, VRF: global

```

```

Reliability 255/255, Txload 1/255, Rxload 1/255
Ethernet address is 0000.5e00.0101
5 minutes input rate 0 bits/sec, 0 packets/sec
5 minutes output rate 0 bits/sec, 0 packets/sec
0 packets received; 1 packets sent
0 multicast packets received
1 multicast packets sent
0 input errors; 0 output errors
0 collisions; 0 dropped
Unknown protocol 0
Spine2#show interface vxlan 200
vxlan200:
line protocol is up
Flags: (0xc008063) BROADCAST MULTICAST ARP RUNNING
Type: ETHERNET_CSMACD
Internet address: 5.0.0.1/24
Broadcast address: 5.0.0.255
Metric: 0, MTU: 1500, BW: 100000 Kbps, DLY: 100 usec, VRF: global
Reliability 255/255, Txload 1/255, Rxload 1/255
Ethernet address is 0000.5e00.0102
5 minutes input rate 0 bits/sec, 0 packets/sec
5 minutes output rate 0 bits/sec, 0 packets/sec
0 packets received; 1 packets sent
0 multicast packets received
1 multicast packets sent
0 input errors; 0 output errors
0 collisions; 0 dropped
Unknown protocol 0

```

```

Spine2#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
U - Per-user Static route
O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

```

```

C 2.0.0.0/24 is directly connected, 02:35:05, vxlan100
O 3.0.0.0/24 [110/2] via 4.0.0.1, 00:45:30, vlan4
C 4.0.0.0/24 is directly connected, 06:08:19, vlan4
C 5.0.0.0/24 is directly connected, 02:08:45, vxlan200
O 6.0.0.0/24 [110/2] via 7.0.0.1, 05:51:24, vlan7
C 7.0.0.0/24 is directly connected, 06:08:01, vlan7
C 127.0.0.0/8 is directly connected, 1d:00:42:19, lo0
O 10.0.0.1/32 [110/2] via 4.0.0.1, 05:51:24, vlan4
C 20.0.0.1/32 is directly connected, 06:09:57, loopback0
O 20.0.1.1/32 [110/3] via 7.0.0.1, 05:11:01, vlan7
[110/3] via 4.0.0.1, 00:00:21, vlan4
C 20.0.2.1/32 is directly connected, 05:13:31, loopback1
O 30.0.0.1/32 [110/2] via 7.0.0.1, 05:51:24, vlan7

```

## Step 8: View the BGP EVPN route and VXLAN session information

### #View the BGP EVPN route information of Leaf1.

```

Leaf1#show bgp l2vpn evpn all all-type
BGP local router ID is 10.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
EVPN Information for Route Distinguisher:100:1
MAC/IP Advertisement Routes:
Network(ETID:MAC:IP) Next Hop Metric LocPrf Weight Path
[B]*>i0:48:0000.5e00.0101:0:0.0.0.0/96 20.0.0.1 0 100 0 i
[B]* i 20.0.0.1 0 100 0 i

```

```

[B]*> 0:48:0010.9400.0002:0:0.0.0/96      0.0.0.0      0      32768 i
[B]*>i:0:48:0000.5e00.0101:32:2.0.0.1/128 20.0.0.1     0      100 0 i
[B]* i      20.0.0.1      0      100 0 i
[B]*> 0:48:0010.9400.0002:32:2.0.0.2/128 0.0.0.0      0      32768 i
Inclusive Multicast Ethernet Tag Routes:
  Network(Originating IP Addr)      Next Hop      Metric  LocPrf Weight Path
[B]*> 0:32:10.0.0.1/72                0.0.0.0      0      32768 i
[B]*>i:0:32:20.0.0.1/72              20.0.0.1     0      100 0 i
[B]* i      20.0.0.1      0      100 0 i

```

### #View the BGP EVPN route information of Leaf2.

```

Leaf2#show bgp l2vpn evpn all all-type
BGP local router ID is 30.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
EVPN Information for Route Distinguisher:200:1
MAC/IP Advertisement Routes:
  Network(ETID:MAC:IP)      Next Hop      Metric  LocPrf Weight Path
[B]*>i:0:48:0000.5e00.0102:0:0.0.0/96     20.0.0.1     0      100 0 i
[B]* i      20.0.0.1     0      100 0 i
[B]*> 0:48:0010.9400.0001:0:0.0.0/96      0.0.0.0      0      32768 i
[B]*>i:0:48:0000.5e00.0102:32:5.0.0.1/128 20.0.0.1     0      100 0 i
[B]* i      20.0.0.1     0      100 0 i
[B]*> 0:48:0010.9400.0001:32:5.0.0.2/128 0.0.0.0      0      32768 i
Inclusive Multicast Ethernet Tag Routes:
  Network(Originating IP Addr)      Next Hop      Metric  LocPrf Weight Path
[B]*>i:0:32:20.0.0.1/72              20.0.0.1     0      100 0 i
[B]* i      20.0.0.1     0      100 0 i
[B]*> 0:32:30.0.0.1/72                0.0.0.0      0      32768 i

```

### #View the BGP EVPN route information of Spine1.

```

Spine1#show bgp l2vpn evpn all all-type
BGP local router ID is 20.0.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
EVPN Information for Route Distinguisher:100:1
MAC/IP Advertisement Routes:
  Network(ETID:MAC:IP)      Next Hop      Metric  LocPrf Weight Path
[B]*> 0:48:0000.5e00.0101:0:0.0.0/96      0.0.0.0      0      32768 i
[B]*>i:0:48:0010.9400.0002:0:0.0.0/96      10.0.0.1     0      100 0 i
[B]*> 0:48:0000.5e00.0101:32:2.0.0.1/128 0.0.0.0      0      32768 i
[B]*>i:0:48:0010.9400.0002:32:2.0.0.2/128 10.0.0.1     0      100 0 i
Inclusive Multicast Ethernet Tag Routes:
  Network(Originating IP Addr)      Next Hop      Metric  LocPrf Weight Path
[B]*>i:0:32:10.0.0.1/72              10.0.0.1     0      100 0 i
[B]*> 0:32:20.0.0.1/72                0.0.0.0      0      32768 i
EVPN Information for Route Distinguisher:200:1
MAC/IP Advertisement Routes:
  Network(ETID:MAC:IP)      Next Hop      Metric  LocPrf Weight Path
[B]*> 0:48:0000.5e00.0102:0:0.0.0/96      0.0.0.0      0      32768 i
[B]*>i:0:48:0010.9400.0001:0:0.0.0/96      30.0.0.1     0      100 0 i
[B]*> 0:48:0000.5e00.0102:32:5.0.0.1/128 0.0.0.0      0      32768 i
[B]*>i:0:48:0010.9400.0001:32:5.0.0.2/128 30.0.0.1     0      100 0 i
Inclusive Multicast Ethernet Tag Routes:
  Network(Originating IP Addr)      Next Hop      Metric  LocPrf Weight Path
[B]*> 0:32:20.0.0.1/72                0.0.0.0      0      32768 i
[B]*>i:0:32:30.0.0.1/72              30.0.0.1     0      100 0 i

```

### #View the tunnel information and VXLAN session of Leaf1.

```
Leaf1#show vxlan tunnel
Reason codes: SI - Source is Invalid:
    source address is not local;
    source interface is down;
    source interface is a tunnel or management interface.
DI - Destination is Invalid:
    destination address is local;
    destination address is unreachable;
    output interface is a tunnel or management interface.
```

```
Number of vxlan tunnel: 1
```

TunnelID	Source	Destination	State
32768	10.0.0.1	20.0.0.1	up

```
Leaf1#show vxlan session
Number of vxlan session: 1
```

VXLAN-ID	SessionID	TunnelID	Source	Destination	State
100	32768	32768	10.0.0.1	20.0.0.1	up

```
Leaf1#show vxlan session 20.0.0.1
```

```
vxlan session 32768
state: up
source IP: 10.0.0.1
destination IP: 20.0.0.1
source mac: 0001.7a91.2de8
destination mac: 0001.7a21.8203
interface: vlan4
switchport: tengigabitethernet0/3
source mac: 0001.7a91.2de8
destination mac: 0001.7a21.81e7
interface: vlan3
switchport: tengigabitethernet0/2
vxlan list: 100
vxlan unicast list: 100
vxlan multicast list: 100
```

You can see that Leaf1 has established dynamic unicast and multicast VXLAN sessions with both Spine1 and Spine2.

#View the tunnel information and VXLAN session of Leaf2.

```
Leaf2#show vxlan tunnel
Reason codes: SI - Source is Invalid:
    source address is not local;
    source interface is down;
    source interface is a tunnel or management interface.
DI - Destination is Invalid:
    destination address is local;
    destination address is unreachable;
    output interface is a tunnel or management interface.
```

```
Number of vxlan tunnel: 1
```

TunnelID	Source	Destination	State
32768	30.0.0.1	20.0.0.1	up

```
Leaf2#show vxlan session
Number of vxlan session: 1
```

```

-----
VXLAN-ID  SessionID  TunnelID  Source      Destination  State
-----
200      32768      32768     30.0.0.1    20.0.0.1    up
Leaf2#show vxlan session 20.0.0.1
vxlan session 32768
state: up
source IP: 30.0.0.1
destination IP: 20.0.0.1
source mac: 0001.7a00.5278
destination mac: 0001.7a21.81e7
interface: vlan6
switchport: tengigabitethernet0/2
source mac: 0001.7a00.5278
destination mac: 0001.7a21.8203
interface: vlan7
switchport: tengigabitethernet0/3
vxlan list: 200
vxlan unicast list: 200
vxlan multicast list: 200

```

It is indicated that Leaf2 has established dynamic unicast and multicast VXLAN sessions with both Spine1 and Spine2.

Step 8: Check the result.

#Configure the gateways on Server1 and Server2.

#Ping Server2 on Server1.

```

C:\Documents and Settings\ Server 1> ping 5.0.0.2

Pinging 5.0.0.2 with 32 bytes of data:

Reply from 5.0.0.2: bytes=32 time<1ms TTL=255

Ping statistics for 5.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0m

```

It is indicated that Server1 and Server2 can be intercommunicated across the three-layer network.

## 126.3.5 Configure BGP EVPN VXLAN Distributed Gateway

### Network Requirements

- Create VXLAN instances on Leaf1 and Leaf2, respectively.
- Leaf1, Spine1, and Leaf2 use MP-IBGP to get through the EVPN route, and Leaf1 and Leaf2 create the IBGP EVPN VXLAN tunnel, and create the VRF instances and VXLAN centralized gateways on Spine1 and Spine2, allowing for intercommunication between Server1 and Server 2 on the same network segment, and between Server2

and Server3 on the different network segments.

- Enable the import of the route to the EVPN address family under the BGP VRF address family on Leaf1 and Leaf2.

## Network Topology

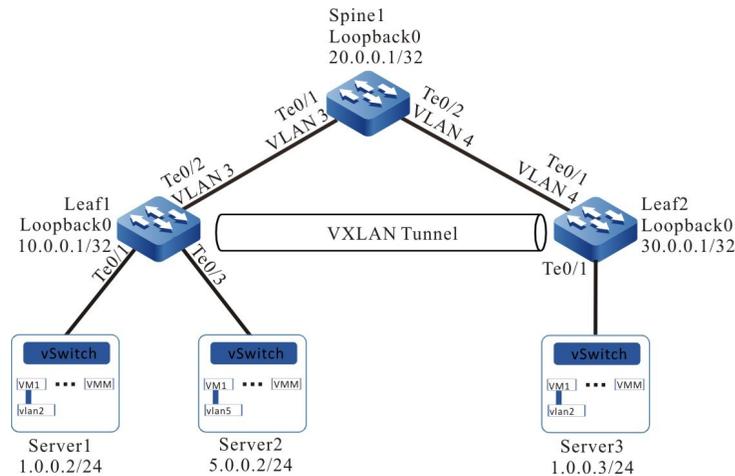


Figure 126-5 Network Topology for Configuring BGP EVPN VXLAN Distributed Gateway

## Configuration Steps

- Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)
- Step 2: Configure IP addresses for the ports.

### #Configure Leaf1.

```
Leaf1(config)#interface loopback 0
Leaf1(config-if-loopback0)#ip address 10.0.0.1 255.255.255.255
Leaf1(config-if-loopback0)#exit
Leaf1(config)#interface loopback 1
Leaf1(config-if-loopback1)#ip address 10.0.1.1 255.255.255.255
Leaf1(config-if-loopback1)#exit
Leaf1(config)#interface vlan 3
Leaf1(config-if-vlan3)#ip address 2.0.0.1 255.255.255.0
Leaf1(config-if-vlan3)#exit
```

### #Configure Spine1.

```
Spine1(config)#interface loopback 0
Spine1(config-if-loopback0)#ip address 20.0.0.1 255.255.255.255
Spine1(config-if-loopback0)#exit
Spine1(config)#interface loopback 1
Spine1(config-if-loopback1)#ip address 20.0.1.1 255.255.255.255
Spine1(config-if-loopback1)#exit
Spine1(config)#interface vlan 3
Spine1(config-if-vlan3)#ip address 2.0.0.2 255.255.255.0
Spine1(config-if-vlan3)#exit
```

```
Spine1(config)#interface vlan 4
Spine1(config-if-vlan4)#ip address 3.0.0.1 255.255.255.0
Spine1(config-if-vlan4)#exit
```

### #Configure Leaf2.

```
Leaf2(config)#interface loopback 0
Leaf2(config-if-loopback0)#ip address 30.0.0.1 255.255.255.255
Leaf2(config-if-loopback0)#exit
Leaf2(config)#interface loopback 1
Leaf2(config-if-loopback1)#ip address 30.0.1.1 255.255.255.255
Leaf2(config-if-loopback1)#exit
Leaf2(config)#interface vlan 4
Leaf2(config-if-vlan4)#ip address 3.0.0.2 255.255.255.0
Leaf2(config-if-vlan4)#exit
```

Step 3: Configure OSPF so that the routes of Loopback between devices are reachable from each other.

### #Configure Leaf1.

```
Leaf1#configure terminal
Leaf1(config)#router ospf 100
Leaf1(config-ospf)#network 10.0.0.1 0.0.0.0 area 0
Leaf1(config-ospf)#network 10.0.1.1 0.0.0.0 area 0
Leaf1(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Leaf1(config-ospf)#exit
```

### #Configure Spine1.

```
Spine1#configure terminal
Spine1(config)#router ospf 100
Spine1(config-ospf)#network 20.0.0.1 0.0.0.0 area 0
Spine1(config-ospf)#network 20.0.1.1 0.0.0.0 area 0
Spine1(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Spine1(config-ospf)#network 3.0.0.0 0.0.0.255 area 0
Spine1(config-ospf)#exit
```

### #Configure Leaf2.

```
Leaf2#configure terminal
Leaf2(config)#router ospf 100
Leaf2(config-ospf)#network 30.0.0.1 0.0.0.0 area 0
Leaf2(config-ospf)#network 30.0.1.1 0.0.0.0 area 0
Leaf2(config-ospf)#network 3.0.0.0 0.0.0.255 area 0
Leaf2(config-ospf)#exit
```

### #View the routing table of Leaf1.

```
Leaf1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 2.0.0.0/24 is directly connected, 00:56:51, vlan3
O 3.0.0.0/24 [110/2] via 2.0.0.2, 00:56:00, vlan3
C 10.0.1.0/24 is directly connected, 00:08:30, loopback1
C 127.0.0.0/8 is directly connected, 3d:03:23:29, lo0
C 10.0.0.1/32 is directly connected, 00:56:51, loopback0
O 20.0.0.1/32 [110/2] via 2.0.0.2, 00:56:00, vlan3
O 20.0.1.1/32 [110/2] via 2.0.0.2, 00:05:22, vlan3
O 30.0.0.1/32 [110/3] via 2.0.0.2, 00:55:52, vlan3
O 30.0.1.1/32 [110/3] via 2.0.0.2, 00:05:44, vlan3
```

## #View the routing table of Spine1.

```
Spine1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 2.0.0.0/24 is directly connected, 01:01:05, vlan3
C 3.0.0.0/24 is directly connected, 01:01:05, vlan4
C 20.0.1.0/24 is directly connected, 00:12:40, loopback1
C 127.0.0.0/8 is directly connected, 1w4d:09:22:41, lo0
O 10.0.0.1/32 [110/2] via 2.0.0.1, 01:00:21, vlan3
O 10.0.1.1/32 [110/2] via 2.0.0.1, 00:08:04, vlan3
C 20.0.0.1/32 is directly connected, 01:01:05, loopback0
O 30.0.0.1/32 [110/2] via 3.0.0.2, 01:00:13, vlan4
O 30.0.1.1/32 [110/2] via 3.0.0.2, 00:10:05, vlan4
```

## #View the routing table of Leaf2.

```
Leaf2#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

O 2.0.0.0/24 [110/2] via 3.0.0.1, 01:04:02, vlan4
C 3.0.0.0/24 is directly connected, 01:04:44, vlan4
C 30.0.0.0/24 is directly connected, 01:04:44, loopback0
C 30.0.1.0/24 is directly connected, 00:15:47, loopback1
C 127.0.0.0/8 is directly connected, 4d:04:40:07, lo0
O 10.0.0.1/32 [110/3] via 3.0.0.1, 01:04:02, vlan4
O 10.0.1.1/32 [110/3] via 3.0.0.1, 00:11:49, vlan4
O 20.0.0.1/32 [110/2] via 3.0.0.1, 01:04:02, vlan4
O 20.0.1.1/32 [110/2] via 3.0.0.1, 00:13:28, vlan4
```

You can see that Leaf1, Spine1 and Leaf2 all have learned the route of the loopback interface of the peer end by running the OSPF protocol.

Step 4: Configure VXLAN and associate VNID, and configure the EVPN address family so that the ports of Leaf1 and Leaf2 are added into VXLAN.

## #Configure Leaf1.

```
Leaf1(config)#vxlان 100
Leaf1(config-vxlان-100)#vxlان vnid 100
Leaf1(config-vxlان-100)#address-family evpn
Leaf1(config-vxlان-evpn)#rd 100:1
Leaf1(config-vxlان-evpn)#route-target both 100:1
Leaf1(config-vxlان-evpn)#exit
Leaf1(config-vxlان-100)#exit
Leaf1(config)# interface tengigabitethernet 0/1
Leaf1(config-if-tengigabitethernet0/1)# vxlان 100 encapsulation vlan 2
Leaf1(config-if-tengigabitethernet0/1)#exit

Leaf1(config)# vxlان 200
Leaf1(config-vxlان-200)#vxlان vnid 200
Leaf1(config-vxlان-200)#address-family evpn
Leaf1(config-vxlان-evpn)#rd 200:1
Leaf1(config-vxlان-evpn)#route-target both 200:1
Leaf1(config-vxlان-evpn)#exit
Leaf1(config-vxlان-200)#exit
```

```
Leaf1(config)# interface tengigabitethernet 0/3
Leaf1(config-if-tengigabitethernet0/3)# vxlan 200 encapsulation vlan 5
Leaf1(config-if-tengigabitethernet0/3)#exit
```

### #Configure Spine1.

```
Spine1(config)#vxlan 100
Spine1(config-vxlan-100)#vxlan vnid 100
Spine1(config-vxlan-100)#address-family evpn
Spine1(config-vxlan-100)#rd 100:1
Spine1(config-vxlan-100)#route-target both 100:1
Spine1(config-vxlan-100)#exit
Spine1(config-vxlan-100)#exit
Spine1(config)#vxlan 200
Spine1(config-vxlan-200)#vxlan vnid 200
Spine1(config-vxlan-200)#address-family evpn
Spine1(config-vxlan-200)#rd 200:1
Spine1(config-vxlan-200)#route-target both 200:1
Spine1(config-vxlan-200)#exit
Spine1(config-vxlan-200)#exit
```

### #Configure Leaf2.

```
Leaf2(config)#vxlan 100
Leaf2(config-vxlan-100)#vxlan vnid 100
Leaf2(config-vxlan-100)#address-family evpn
Leaf2(config-vxlan-100)#rd 100:1
Leaf2(config-vxlan-100)#route-target both 100:1
Leaf2(config-vxlan-100)#exit
Leaf2(config-vxlan-100)#exit
Leaf2(config)# interface tengigabitethernet 0/1
Leaf2(config-if-tengigabitethernet0/1)# vxlan 100 encapsulation vlan 2
Leaf2(config-if-tengigabitethernet0/1)#exit
```

### #View the VXLAN information of Leaf1.

```
Leaf1#show vxlan config

vxlan 100
vxlan vnid 100
address-family evpn
rd 100:1
route-target import 100:1
route-target export 100:1
exit
exit
vxlan 200
vxlan vnid 200
address-family evpn
rd 200:1
route-target import 200:1
route-target export 200:1
exit
exit
Leaf1#show running-config interface te0/1

interface tengigabitethernet0/1
switchport mode trunk
switchport trunk allowed vlan add 2
switchport trunk pvid vlan 10
vxlan 100 encapsulation vlan 2
exit
```

```
Leaf1#show running-config interface te0/3

interface tengigabitethernet0/3
 switchport mode trunk
 switchport trunk allowed vlan add 5
 switchport trunk pvid vlan 10
 vxlan 200 encapsulation vlan 5
 exit
```

#### #View the VXLAN information of Spine1.

```
Spine1#show vxlan config

vxlan 100
 vxlan vniid 100
 address-family evpn
  rd 100:1
  route-target import 100:1
  route-target export 100:1
 exit
exit
vxlan 200
 vxlan vniid 200
 address-family evpn
  rd 200:1
  route-target import 200:1
  route-target export 200:1
 exit
exit
```

#### #View the VXLAN information of Leaf2.

```
Leaf2#show vxlan config

vxlan 100
 vxlan vniid 100
 address-family evpn
  rd 100:1
  route-target import 100:1
  route-target export 100:1
 exit
exit
Leaf1#show running-config interface te0/1

interface tengigabitethernet0/1
 switchport mode trunk
 switchport trunk allowed vlan add 2
 switchport trunk pvid vlan 10
 vxlan 100 encapsulation vlan 2
 exit
```

#### Step 5: Configure BGP.

#### #Configure Leaf1.

Configure to establish the IBGP peer to Spine1, and activate the advertising capability under the EVPN address family

```
Leaf1(config)#router bgp 100
Leaf1(config-bgp)#neighbor 20.0.1.1 remote-as 100
Leaf1(config-bgp)#neighbor 20.0.1.1 update-source loopback 1
```

```

Leaf1(config-bgp)#address-family l2vpn evpn
Leaf1(config-bgp-af)#neighbor 20.0.1.1 activate
Leaf1(config-bgp-af)#exit-address-family
Leaf1(config-bgp)#exit

```

### #Configure Spine1.

Configure to establish the IBGP peers respectively to Leaf1 and Leaf2, and activate the advertising capability and configuration reflector under the EVPN address family.

```

Spine1(config)#router bgp 100
Spine1(config-bgp)#neighbor 10.0.1.1 remote-as 100
Spine1(config-bgp)#neighbor 10.0.1.1 update-source loopback 1
Spine1(config-bgp)#neighbor 30.0.1.1 remote-as 100
Spine1(config-bgp)#neighbor 30.0.1.1 update-source loopback 1
Spine1(config-bgp)#address-family l2vpn evpn
Spine1(config-bgp-af)#neighbor 10.0.1.1 activate
Spine1(config-bgp-af)#neighbor 10.0.1.1 route-reflector-client
Spine1(config-bgp-af)#neighbor 30.0.1.1 activate
Spine1(config-bgp-af)#neighbor 30.0.1.1 route-reflector-client
Spine1(config-bgp-af)#exit-address-family
Spine1(config-bgp)#exit

```

### #Configure Leaf2.

Configure to establish the IBGP peer to Spine1, and activate the advertising capability under the EVPN address family.

```

Leaf2(config)#router bgp 100
Leaf2(config-bgp)#neighbor 20.0.1.1 remote-as 100
Leaf2(config-bgp)#neighbor 20.0.1.1 update-source loopback 1
Leaf2(config-bgp)#address-family l2vpn evpn
Leaf2(config-bgp-af)#neighbor 20.0.1.1 activate
Leaf2(config-bgp-af)#exit-address-family
Leaf2(config-bgp)#exit

```

### #Check BGP EVPN neighbors of Leaf1.

```

Leaf1#show bgp l2vpn evpn summary
BGP router identifier 10.0.1.1, local AS number 100
BGP table version is 1
 1 BGP AS-PATH entries
 0 BGP community entries

Neighbor    V    AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State/PfxRed
20.0.1.1    4    100    2    2    1    0  0 00:00:28    0

Total number of neighbors 1

```

### #Check BGP EVPN neighbors of Spine1.

```

Spine1#show bgp l2vpn evpn summary
BGP router identifier 20.0.1.1, local AS number 100
BGP table version is 1
 1 BGP AS-PATH entries
 0 BGP community entries

Neighbor    V    AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State/PfxRed
10.0.1.1    4    100    3    3    1    0  0 00:01:34    0
30.0.1.1    4    100    2    2    1    0  0 00:00:02    0

Total number of neighbors 2

```

## #Check BGP EVPN neighbors of Leaf2.

```
Leaf2#show bgp l2vpn evpn summary
BGP router identifier 30.0.1.1, local AS number 100
BGP table version is 1
1 BGP AS-PATH entries
0 BGP community entries

Neighbor    V    AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State/PfxRcd
20.0.1.1    4    100   3     3     1     0  0:00:01:10    0

Total number of neighbors 1
```

## Step 6: Configure the VRF instance

### #Configure the VRF instance of Leaf1.

```
Leaf1(config)#ip vrf 1
Leaf1(config-vrf)#rd 100:2
Leaf1(config-vrf)#l3vnid 1
Leaf1(config-vrf)#address-family evpn
Leaf1(config-vrf-evpn)#route-target both 100:2
Leaf1(config-vrf-evpn)#exit
Leaf1(config-vrf)#exit
```

### #Configure the VRF instance of Leaf2.

```
Leaf2(config)#ip vrf 1
Leaf2(config-vrf)#rd 100:2
Leaf2(config-vrf)#l3vnid 1
Leaf2(config-vrf)#address-family evpn
Leaf2(config-vrf-evpn)#route-target both 100:2
Leaf2(config-vrf-evpn)#exit
Leaf2(config-vrf)#exit
```

## Step 7: Create the NVE interface

### #Configure the NVE interface of Leaf1 and configure the corresponding VXLAN to use the BGP protocol to dynamically establish a L2 tunnel.

```
Leaf1(config)#interface nve 1
Leaf1(config-if-nve1)#source 10.0.0.1
Leaf1(config-if-nve1)#vxlan 100,200 ingress-replication protocol bgp
Leaf1(config-if-nve1)#mac-address learning disable
Leaf1(config-if-nve1)#exit
```

### #Configure the NVE interface of Leaf2 and configure the corresponding VXLAN to use the BGP protocol to dynamically establish a L2 tunnel.

```
Leaf2(config)#interface nve 1
Leaf2(config-if-nve1)#source 30.0.0.1
Leaf2(config-if-nve1)#vxlan 100 ingress-replication protocol bgp
Leaf2(config-if-nve1)#mac-address learning disable
Leaf2(config-if-nve1)#exit
```

## Step 8: Configure the VXLAN L3 gateway and bind the corresponding VRF instance

### #Configure the L3 gateway of Leaf1 and bind the corresponding VRF instance

```
Leaf1(config)#interface vxlan 200
Leaf1(config-if-vxlan200)#ip vrf forwarding 1
Leaf1(config-if-vxlan200)#vxlan distribute-gateway
Leaf1(config-if-vxlan200)#ip address 5.0.0.1 24
Leaf1(config-if-vxlan200)#exit
```

#Configure the L3 gateway of Leaf2 and bind the corresponding VRF instance.

```
Leaf2(config)#interface vxlan 100
Leaf2(config-if-vxlan100)#ip vrf forwarding 1
Leaf2(config-if-vxlan100)#vxlan distribute-gateway
Leaf2(config-if-vxlan100)#ip address 1.0.0.1 24
Leaf2(config-if-vxlan100)#exit
```

#View the interface VXLAN interface and routing table of Leaf1.

```
Leaf1#show interface vxlan 200
vxlan200:
  line protocol is up
  Flags: (0xc008063) BROADCAST MULTICAST ARP RUNNING
  Type: ETHERNET_CSMACD
  Internet address: 5.0.0.1/24
  Broadcast address: 5.0.0.255
  Metric: 0, MTU: 1500, BW: 100000 Kbps, DLY: 100 usec, VRF: 1
  Reliability 255/255, Txload 1/255, Rxload 1/255
  Ethernet address is 0001.7a00.5278
  5 minutes input rate 0 bits/sec, 0 packets/sec
  5 minutes output rate 0 bits/sec, 0 packets/sec
  94 packets received; 88 packets sent
  0 multicast packets received
  5 multicast packets sent
  0 input errors; 0 output errors
  0 collisions; 0 dropped
  Unknown protocol 0

Leaf1#show ip route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 5.0.0.0/24 is directly connected, 00:01:13, vxlan200
```

#View the tunnel information and the VXLAN session of Leaf2.

```
Leaf2#show interface vxlan 100
vxlan100:
  line protocol is up
  Flags: (0xc008063) BROADCAST MULTICAST ARP RUNNING
  Type: ETHERNET_CSMACD
  Internet address: 1.0.0.1/24
  Broadcast address: 1.0.0.255
  Metric: 0, MTU: 1500, BW: 100000 Kbps, DLY: 100 usec, VRF: 1
  Reliability 255/255, Txload 1/255, Rxload 1/255
  Ethernet address is 0001.7a6a.0042
  5 minutes input rate 0 bits/sec, 0 packets/sec
  5 minutes output rate 0 bits/sec, 0 packets/sec
  0 packets received; 2 packets sent
  0 multicast packets received
  2 multicast packets sent
  0 input errors; 0 output errors
  0 collisions; 0 dropped
  Unknown protocol 0

Leaf2#show ip route vrf 1
```

Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS  
 U - Per-user Static route  
 O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 1.0.0.0/24 is directly connected, 00:02:15, vxlan100

### #View the tunnel information and the VXLAN session of Leaf1

```
Leaf1#show vxlan tunnel
Reason codes: SI - Source is Invalid:
    source address is not local;
    source interface is down;
    source interface is a tunnel or management interface.
DI - Destination is Invalid:
    destination address is local;
    destination address is unreachable;
    output interface is a tunnel or management interface.
```

Number of vxlan tunnel: 1

TunnelID	Source	Destination	State
32768	10.0.0.1	30.0.0.1	up

```
Leaf1#show vxlan session
Number of vxlan session: 1
```

VXLAN-ID	SessionID	TunnelID	Source	Destination	State
100	32768	32768	10.0.0.1	30.0.0.1	up

```
Leaf1#show vxlan session l3
Number of vxlan session: 1
```

VXLAN-ID	SessionID	TunnelID	Source	Destination	State
8191	32768	32768	10.0.0.1	30.0.0.1	up

### #View the tunnel information and VXLAN session of Leaf2.

```
Leaf2#show vxlan tunnel
Reason codes: SI - Source is Invalid:
    source address is not local;
    source interface is down;
    source interface is a tunnel or management interface.
DI - Destination is Invalid:
    destination address is local;
    destination address is unreachable;
    output interface is a tunnel or management interface.
```

Number of vxlan tunnel: 1

TunnelID	Source	Destination	State
32768	30.0.0.1	10.0.0.1	up

```
Leaf2#show vxlan session
Number of vxlan session: 1
```

VXLAN-ID	SessionID	TunnelID	Source	Destination	State
100	32768	32768	30.0.0.1	10.0.0.1	up

```
Leaf2#show vxlan session l3
Number of vxlan session: 1

-----
VXLAN-ID  SessionID  TunnelID  Source      Destination  State
-----
8191      32768      32768     30.0.0.1    10.0.0.1     up
```

From the information described above, you can see that the tunnel is UP, and the dynamic VXLAN session can be normally established.

Step 9: Configure the VRF unicast route and enable the function of importing the route into the EVPN address family under the BGP VRF address family.

#Configure Leaf1.

```
Leaf1(config)#interface loopback 2
Leaf1(config-if-loopback2)#ip vrf forwarding 1
Leaf1(config-if-loopback2)#ip address 11.0.0.1 255.255.255.255
Leaf1(config-if-loopback2)#exit
Leaf1(config)#router bgp 100
Leaf1(config-bgp)#address-family ipv4 vrf 1
Leaf1(config-bgp-af)#advertise-l2vpn-evpn
Leaf1(config-bgp-af)#network 11.0.0.1 255.255.255.255
Leaf1(config-bgp-af)#exit-address-family
Leaf1(config-bgp)#exit
```

#Configure Leaf2.

```
Leaf2(config)#interface loopback 2
Leaf2(config-if-loopback2)#ip vrf forwarding 1
Leaf2(config-if-loopback2)#ip address 31.0.0.1 32
Leaf2(config-if-loopback2)#exit
Leaf2(config)#router bgp 100
Leaf2(config-bgp)#address-family ipv4 vrf 1
Leaf2(config-bgp-af)#advertise-l2vpn-evpn
Leaf2(config-bgp-af)#network 31.0.0.1 255.255.255.255
Leaf2(config-bgp-af)#exit-address-family
Leaf2(config-bgp)#exit
```

#Server1、Server2 and Server3 send the arp.

#View the category 2 and category 5 BGP EVPN routes and VRF unicast route of Leaf1.

```
Leaf1#show bgp l2vpn evpn all type 2
BGP local router ID is 10.0.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
EVPN Information for Route Distinguisher: 100:1
MAC/IP Advertisement Routes:
Network(ETID:MAC:IP)          Next Hop      Metric  LocPrf Weight Path
[B]*>i:48:0001.7a6a.0042:0:0.0.0/96      30.0.0.1      0      100   0 i
[B]*> 0:48:0010.9400.104c:0:0.0.0/96      0.0.0.0       0      32768 i
[B]*>i:48:0010.9400.104e:0:0.0.0/96      30.0.0.1      0      100   0 i
[B]*>i:48:0001.7a6a.0042:32:1.0.0.1/128   30.0.0.1      0      100   0 i
[B]*> 0:48:0010.9400.104c:32:1.0.0.2/128  0.0.0.0       0      32768 i
[B]*>i:48:0010.9400.104e:32:1.0.0.3/128  30.0.0.1      0      100   0 i
EVPN Information for Route Distinguisher: 100:2
MAC/IP Advertisement Routes:
Network(ETID:MAC:IP)          Next Hop      Metric  LocPrf Weight Path
[B]*>i:48:0001.7a6a.0042:32:1.0.0.1/128  30.0.0.1      0      100   0 i
```

```

[B]*>i0:48:0010.9400.104e:32:1.0.0.3/128      30.0.0.1      0      100      0 i
EVPN Information for Route Distinguisher:200:1
MAC/IP Advertisement Routes:
  Network(ETID:MAC:IP)      Next Hop      Metric      LocPrf Weight Path
[B]*> 0:48:0001.7a00.5278:0:0.0.0.0/96      0.0.0.0      0      32768 i
[B]*> 0:48:0010.9400.104d:0:0.0.0.0/96      0.0.0.0      0      32768 i
[B]*> 0:48:0001.7a00.5278:32:5.0.0.1/128      0.0.0.0      0      32768 i
[B]*> 0:48:0010.9400.104d:32:5.0.0.2/128      0.0.0.0      0      32768 i

Leaf1#show bgp l2vpn evpn all type 5
BGP local router ID is 10.0.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
EVPN Information for Route Distinguisher:100:2
IP Prefix Routes:
  Network(ETID:IP)      Next Hop      Metric      LocPrf Weight Path
[B]*> 0:32:11.0.0.1/72      0.0.0.0      0      32768 i
[B]*>i0:32:31.0.0.1/72      30.0.0.1      0      100      0 i

Leaf1#show ip route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 5.0.0.0/24 is directly connected, 00:09:00, vxlan200
B 1.0.0.1/32 [200/0] via 30.0.0.1, 00:06:31, vxlan4097
B 1.0.0.3/32 [200/0] via 30.0.0.1, 00:01:48, vxlan4097
C 11.0.0.1/32 is directly connected, 00:08:47, loopback2
B 31.0.0.1/32 [200/0] via 30.0.0.1, 00:06:17, vxlan4097

```

## #View the category 2 and category 5 BGP EVPN routes and VRF unicast route of Leaf2.

```

Leaf2#show bgp l2vpn evpn all type 2
BGP local router ID is 30.0.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
EVPN Information for Route Distinguisher:100:1
MAC/IP Advertisement Routes:
  Network(ETID:MAC:IP)      Next Hop      Metric      LocPrf Weight Path
[B]*> 0:48:0001.7a6a.0042:0:0.0.0.0/96      0.0.0.0      0      32768 i
[B]*>i0:48:0010.9400.104c:0:0.0.0.0/96      10.0.0.1      0      100      0 i
[B]*> 0:48:0010.9400.104e:0:0.0.0.0/96      0.0.0.0      0      32768 i
[B]*> 0:48:0001.7a6a.0042:32:1.0.0.1/128      0.0.0.0      0      32768 i
[B]*>i0:48:0010.9400.104c:32:1.0.0.2/128      10.0.0.1      0      100      0 i
[B]*> 0:48:0010.9400.104e:32:1.0.0.3/128      0.0.0.0      0      32768 i
EVPN Information for Route Distinguisher:100:2
MAC/IP Advertisement Routes:
  Network(ETID:MAC:IP)      Next Hop      Metric      LocPrf Weight Path
[B]*>i0:48:0001.7a00.5278:32:5.0.0.1/128      10.0.0.1      0      100      0 i
[B]*>i0:48:0010.9400.104d:32:5.0.0.2/128      10.0.0.1      0      100      0 i
EVPN Information for Route Distinguisher:200:1
MAC/IP Advertisement Routes:
  Network(ETID:MAC:IP)      Next Hop      Metric      LocPrf Weight Path
[B]*>i0:48:0001.7a00.5278:32:5.0.0.1/128      10.0.0.1      0      100      0 i
[B]*>i0:48:0010.9400.104d:32:5.0.0.2/128      10.0.0.1      0      100      0 i

Leaf2#show bgp l2vpn evpn all type 5
BGP local router ID is 30.0.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

```

```

EVPN Information for Route Distinguisher:100:2
IP Prefix Routes:
  Network(ETID:IP)           Next Hop      Metric  LocPrf Weight Path
[B]*>i0:32:11.0.0.1/72      10.0.0.1     0       100   0  i
[B]*> 0:32:31.0.0.1/72     0.0.0.0      0       32768 i
Leaf2#
Leaf2#show ip rou
Leaf2#show ip route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
        U - Per-user Static route
        O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 1.0.0.0/24 is directly connected, 00:09:10, vxlan100
B 5.0.0.1/32 [200/0] via 10.0.0.1, 00:08:31, vxlan4097
B 5.0.0.2/32 [200/0] via 10.0.0.1, 00:08:31, vxlan4097
B 11.0.0.1/32 [200/0] via 10.0.0.1, 00:08:31, vxlan4097
C 31.0.0.1/32 is directly connected, 00:09:14, loopback2

```

From the information described above, you can see that the device normally learns the VRF unicast route through the EVPN route.

Step 10: Check the result.

#Ping Server1 on Server3.

```

C:\Documents and Settings\ Server 3> ping 1.0.0.2

Pinging 1.0.0.2 with 32 bytes of data:

Reply from 1.0.0.2: bytes=32 time<1ms TTL=255

Ping statistics for 1.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0m

```

You can see that Server1 and Server3 can be intercommunicated across the three-layer network between Leaf1, Spine1 and Leaf2.

#Ping Server2 on Server3.

```

C:\Documents and Settings\ Server 3> ping 5.0.0.2

Pinging 5.0.0.2 with 32 bytes of data:

Reply from 5.0.0.2: bytes=32 time<1ms TTL=255

Ping statistics for 5.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0m

```

It is indicated that Server2 and Server3 can be intercommunicated across the three-layer network between Leaf1, Spine1 and Leaf2.

## 126.3.6 Configure BGP EVPN Cross-Data Center Distributed Gateway

### Network Requirements

- Run the IGP protocol between Spine1, Spine2, Device1, and Device2 to get through the route.
- Run the EBGP protocol between Spine1 and Spine2 to get through the EVPN route, and run the IBGP protocol between Spine1 and Leaf1, and between Spine2 and Leaf2 to get through the EVPN route.
- With Leaf1 and Leaf2 as VTEPs, create the IBGP EVPN VXLAN tunnel, and create the VRF instances and VXLAN distributed gateways on Leaf1 and Leaf2, allowing for intercommunication between Server1 and Server 3 on the same network segment, between Server2 and Server4 on the same network segment, between Server1 and Server4 on the different network segments, and between Server2 and Server3 on the different network segments.
- Enable the import of the route to the EVPN address family under the BGP VRF address family on Leaf1 and Leaf2.

### Network Topology

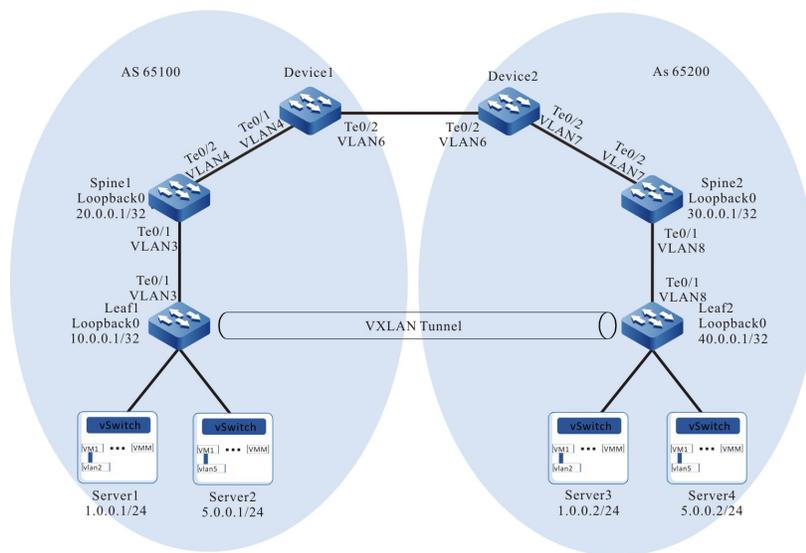


Figure 126-6 Network Topology for Configuring BGP EVPN Cross-Data Center Distributed Gateway

### Configuration Steps

- Step 1: Configure VLANs, and add ports to the required VLANs. (Omitted)
- Step 2: Configure IP addresses for the ports. (Omitted)

Step 3: Configure OSPF so that the routes of Loopback between devices are reachable from each other. (Omitted)

Step 4: Configure VXLAN and associate VNID on Leaf1 and Leaf2, and configure the EVPN address family so that the ports of Leaf1 and Leaf2 are added into VXLAN. (Omitted)

Step 5: Configure BGP.

#Configure Leaf1 to establish the IBGP neighbors to Spine1 and Leaf2, and activate the advertising capability under the EVPN address family. (Omitted)

#Configure Spine1 to establish the EBGP neighbors to Spine2, and activate the advertising capability under the EVPN address family and configure the function of not changing the route attributes when advertising the routes to the neighbors. (Omitted)

Step 6: Configure the VRF instance

#Configure the VRF instances of and Leaf1 and Leaf2. (Omitted)

Step 7: Create the NVE interface

#Configure the NVE interfaces of and Leaf1 and Leaf2 and configure the corresponding VXLAN to use the BGP protocol to dynamically establish a L2 tunnel. (Omitted)

Step 8: #Configure the VXLAN L3 gateways on Leaf1 and Leaf2 and bind the corresponding VRF instances (omitted)

Step 9: Configure the VRF unicast routes on Leaf1 and Leaf2 and enable the function of importing the routes into the EVPN address family under the BGP VRF address family. (Omitted)

Step 10: Check the result.

#Ping Server3 on Server1.

You can see that Server1 and Server3 can be intercommunicated across the three-layer network between Leaf1, Spine1 and Leaf2.

#Ping Server4 on Server1.

It is indicated that Server2 and Server3 can be intercommunicated across the three-layer network between Leaf1, Spine1 and Leaf2.



- 
- For all configurations and result checks in this section, please refer to section 2.3.5.
- 

# 127 NLB

---

## 127.1 Overview

NLB is a multi-server cluster load balancing feature developed by Microsoft on Windows Server. When a switch is connected to an NLB server cluster, the NLB server requires the switch to be able to send the packet whose destination IP address is the IP address of the NLB server cluster to each server in the NLB server cluster.

## 127.2 NLB Function Configuration

Table 127-1 NLB Function Configuration List

Configuration Task	
Configure NLB function	Configure the serviceloop group
	Configure the static ARP to bind the serviceloop group
	Configure the static MAC multiport

### 127.2.1 Configure NLB

#### Configuration Condition

None

#### Configure the Static ARP to Bind the Serviceloop Group

Table 127-2 Configuring the Static ARP to Bind the Serviceloop Group

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the static ARP to bind the servicoop group	<b>arp [ vrf vrf-name ] { ip-address   host-name } mac-address vlan vlan-id servicoop-group servicoop-group-id</b>	Mandatory

## Note

- When using the NLB function, you need to shut down [arp smac-check multicast](#).

### Configure the Static MAC Multiport

With static forwarding MAC address entries configured for multiple egress ports, after receiving packets within the corresponding VLAN, the ports matches the destination MAC addresses of the packets with the static forwarding MAC address entries that are configured on the device.

If they match successfully, the device forwards the packets through the multiple designated egress ports. This function enables the packets to be sent more flexibly

to the multiple egress ports, allowing for multi-forwarding of traffic

Table 127-3 Configuring Static Forwarding MAC Addresses That are Bound to Multiple Egress Ports

Step	Command	Description
Enter the global configuration mode.	<b>config terminal</b>	-
Configure static forwarding MAC addresses that are bound to an aggregation group.	<b>mac-address multiport mac-address-value vlan vlan-id interface { interface-name1 [ to interface-name2 ] }</b>	Mandatory  By default, no static forwarding MAC address of the multiple egress ports is configured in the device

## 127.2.2NLB Monitoring and Maintaining

Table 127-4 NLB Monitoring and Maintaining

Command	Description
<b>show mac-address multiport</b>	Show MAC multiport information
<b>show arp</b>	Show ARP information
<b>show serviceloop-group</b>	Show serviceloop group information

## 127.3 Typical Configuration Example of NLB

### Network Requirements

- After the serviceloop group, MAC multiport, and static ARP are configured, the packets sent from PC will be sent to all NLB servers

### Network Topology

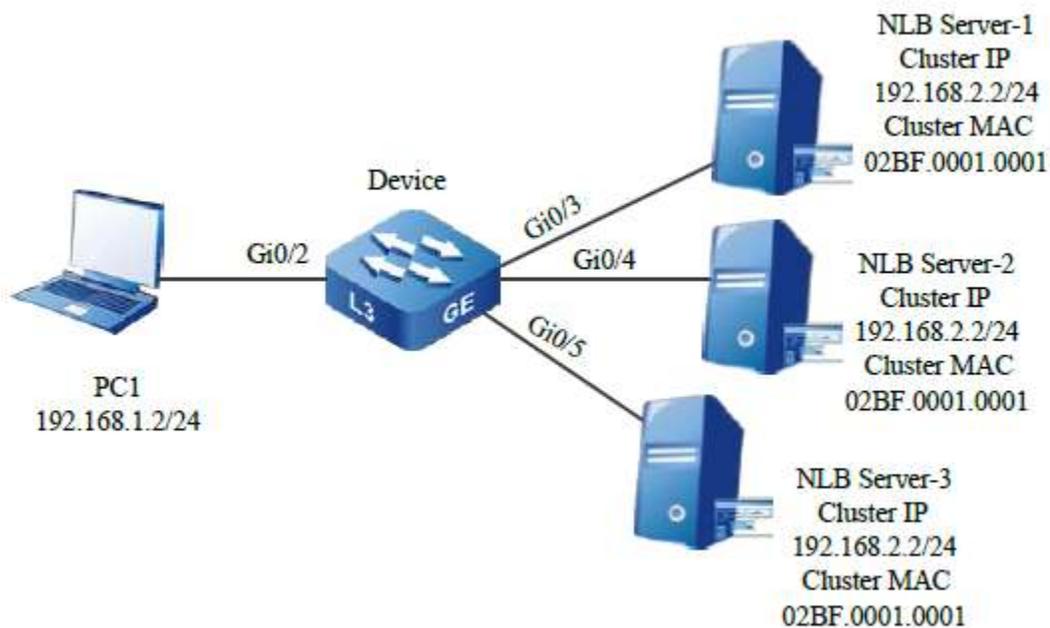


Figure 127-1 Network Topology for Configuring NLB

## Configuration Steps

Step 1: Configure link types and IP addresses of VLANs and ports on Device.

#Create VLAN2 and VLAN3 on Device.

```
Device#configure terminal
Device(config)#vlan
```

2,3

#Configure the link type of port gigabitethernet0/2 as Access to allow the VLAN2 services to pass, enable interfere vlan2, and configure the IP address as 192.168.1.1/24

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode access
Device(config-if-gigabitethernet0/2)#switchport access vlan 2
Device(config-if-gigabitethernet0/2)#exit
Device(config)#interface vlan 2
Device(config-if-vlan2)#ip address 192.168.1.1 255.255.255.0
Device(config-if-vlan2)#exit
```

#Configure the port link type on gigabitethernet 0/3-gigabitethernet 0/5 of Device as Access to allow VLAN3 services to pass, enable interfere vlan3, and configure the IP address as 192.168.2.1/24 (omitted)

Step 2: Configure the serviceloop group

#Configure serviceloop group 1, and select and add any port of the device into this serviceloop group.

```
Device(config)#serviceloop-group 1
Device (config)# interface gigabitethernet 0/6
Device(config-if-gigabitethernet0/6)#serviceloop-group 1 active
Device(config-if-gigabitethernet0/6)#exit
```

Step 3: Configure the MAC multiport.

#Configure the MAC multiport on Device, and designate the egresses as gi0/3-gi0/5

```
Device#configure terminal
Device(config)#mac-address multiport 02BF.1.1 vlan 3 interface gigabitethernet 0/3,0/4,0/5
Device(config)#exit
```

Step 4: Configure static ARP

#Configure the static ARP on Device and bind the serviceloop group

```
Device#configure terminal
Device(config)# arp 192.168.2.2 02bf.1.1 vlan 3 serviceloop-group 1
Device(config)#exit
```

Step 5: Check the result.

## #View the serviceloop group

```
Device# show serviceloop-group
serviceloop group 1
Description:
Number of ports in total: 1
Serviceloop-port: gigabitethernet0/6
```

## #View the MAC multiport

```
Device# show mac-address multiport
mac      vlan      interface
02BF.0001.0001 3      gi0/3-0/5
```

## #View ARP

```
Device# show arp
Protocol Address      Age (min) Hardware Addr  Type  Interface      Switchport
Internet 192.168.1.1   -      0001.7a6a.011e  ARPA  vlan2          ---
Internet 192.168.2.1   -      0001.7a6a.011e  ARPA  vlan3          ---
Internet 192.168.2.2   -      02bf.0001.0001  ARPA  vlan3          gigabitethernet0/3
Internet 192.168.2.2   -      02bf.0001.0001  ARPA  vlan3          gigabitethernet0/4
Internet 192.168.2.2   -      02bf.0001.0001  ARPA  vlan3          gigabitethernet0/5
```

#When the NLB server cluster IP is accessed from PC, each server can receive this packet.