

## 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.
Keywords of Screen print	The red information represents the key information in the screen output.

#### Icon and Symbol Conventions



FORMAT	Description
 说明:	Supplements or emphasizes the foregoing information.
 注意:	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.
 警告:	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.

FORMAT	Description
"<"	
Boldface square brackets " <b>【】</b> "	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.
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>12</b>
<b>1.1</b>	<b>OVERVIEW .....</b>	<b>12</b>
<b>1.2</b>	<b>SYSTEM OPERATION BASIC FUNCTIONS.....</b>	<b>12</b>
1.2.1	DEVICE CONFIGURATION MODE .....	12
1.2.2	COMMAND OPERATING MODE .....	13
1.2.3	COMMAND LINE INTERFACE.....	15
<b>2</b>	<b>SYSTEM LOGIN .....</b>	<b>20</b>
<b>2.1</b>	<b>OVERVIEW .....</b>	<b>20</b>
<b>2.2</b>	<b>SYSTEM LOGIN FUNCTION CONFIGURATION .....</b>	<b>20</b>
2.2.1	LOGGING IN TO THE DEVICE THROUGH THE CONSOLE PORT.....	21
2.2.2	CONFIGURING REMOTE LOGIN THROUGH TELNET .....	23
2.2.3	CONFIGURING REMOTE LOGIN THROUGH SSH .....	24
2.2.4	CONFIGURE REMOTE LOGIN THROUGH WEB.....	26
2.2.5	SYSTEM LOGIN MONITORING AND MAINTAINING .....	28
<b>2.3</b>	<b>TYPICAL CONFIGURATION OF SYSTEM LOGIN EXAMPLE. ....</b>	<b>28</b>
2.3.1	CONFIGURE A LOCAL TERMINAL TO TELNET TO THE DEVICE. ....	28
2.3.2	CONFIGURE A LOCAL DEVICE TO LOG IN TO A REMOTE DEVICE VIA TELNET .....	30
2.3.3	CONFIGURE A LOCAL DEVICE TO LOG IN TO A REMOTE DEVICE VIA SSH .....	31
2.3.4	CONFIGURE A DEVICE AS AN SFTP CLIENT .....	32
2.3.5	CONFIGURE A DEVICE AS AN SFTP SERVER .....	34
2.3.6	CONFIGURE A LOCAL DEVICE TO LOG IN TO A REMOTE DEVICE VIA SSH PUBLIC KEY AUTHENTICATION .....	35
<b>3</b>	<b>SYSTEM CONTROL AND MANAGEMENT .....</b>	<b>41</b>
<b>3.1</b>	<b>OVERVIEW .....</b>	<b>41</b>
<b>3.2</b>	<b>LOGIN CONTROL AND MANAGEMENT FUNCTION CONFIGURATION .....</b>	<b>41</b>
3.2.1	SWITCH OVER BETWEEN USER LEVELS. ....	42
3.2.2	CONFIGURE THE COMMAND LEVEL.....	44
3.2.3	CONFIGURE THE ENABLE PASSWORD. ....	45
3.2.4	CONFIGURE LINE PROPERTIES. ....	45

3.2.5	SYSTEM CONTROL AND MANAGEMENT MONITORING AND MAINTAINING .....	51
<b>4</b>	<b>FTP, FTPS, TFTP AND SFTP.....</b>	<b>52</b>
<b>4.1</b>	<b>OVERVIEW .....</b>	<b>52</b>
<b>4.2</b>	<b>FTP, FTPS, TFTP AND SFTP FUNCTION CONFIGURATION .....</b>	<b>53</b>
4.2.1	CONFIGURE AN FTP SERVER.....	53
4.2.2	CONFIGURE AN FTP CLIENT.....	54
4.2.3	CONFIGURE A TFTP CLIENT.....	55
4.2.4	CONFIGURE THE TFTP SERVER .....	56
4.2.5	CONFIGURE AN SFTP SERVER .....	57
4.2.6	CONFIGURE AN SFTP CLIENT. ....	57
4.2.7	FTP AND TFTP MONITORING AND MAINTAINING .....	58
<b>4.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF FTP AND TFTP.....</b>	<b>58</b>
4.3.1	CONFIGURE A DEVICE AS AN FTP CLIENT .....	58
4.3.2	CONFIGURE A DEVICE AS AN FTP SERVER.....	59
4.3.3	CONFIGURE A DEVICE AS AN TFTP CLIENT.....	63
4.3.4	CONFIGURE A DEVICE AS AN SFTP CLIENT .....	64
4.3.5	CONFIGURE A DEVICE AS AN SFTP SERVER .....	65
4.3.6	CONFIGURE A DEVICE AS AN FTPS CLIENT .....	67
<b>5</b>	<b>FILE SYSTEM MANAGEMENT .....</b>	<b>71</b>
<b>5.1</b>	<b>OVERVIEW .....</b>	<b>71</b>
<b>5.2</b>	<b>FILE SYSTEM MANAGEMENT FUNCTION CONFIGURATION .....</b>	<b>71</b>
5.2.1	MANAGE STORAGE DEVICES.....	72
5.2.2	MANAGE FILE DIRECTORIES.....	73
5.2.3	MANAGE FILE OPERATIONS.....	75
5.2.4	DOWNLOAD A FILE FROM FTP.....	77
5.2.5	CONFIGURE STARTUP PARAMETERS. ....	78
5.2.6	FILE SYSTEM MANAGING, MONITORING, AND MAINTAINING.....	78
<b>5.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF FILE SYSTEM MANAGEMENT .....</b>	<b>79</b>
5.3.1	CONFIGURE STARTUP PARAMETERS. ....	79
<b>6</b>	<b>CONFIGURATION FILE MANAGEMENT.....</b>	<b>80</b>

<b>6.1</b>	<b>OVERVIEW .....</b>	<b>80</b>
<b>6.2</b>	<b>CONFIGURATION FILE MANAGEMENT FUNCTION CONFIGURATION .....</b>	<b>81</b>
6.2.1	SAVE THE CURRENT CONFIGURATION. ....	81
6.2.2	CONFIGURE THE BACKUP SYSTEM .....	82
6.2.3	RESTORE THE STARTUP CONFIGURATION. ....	83
6.2.4	CONFIGURATION FILE MANAGING, MONITORING, AND MAINTAINING .....	84
6.2.5	CONFIGURATION FILE ENCRYPTION .....	84
<b>7</b>	<b>SYSTEM MANAGEMENT .....</b>	<b>85</b>
<b>7.1</b>	<b>OVERVIEW .....</b>	<b>85</b>
<b>7.2</b>	<b>SYSTEM MANAGEMENT FUNCTION CONFIGURATION .....</b>	<b>86</b>
7.2.1	CONFIGURE THE DEVICE NAME.....	86
7.2.2	CONFIGURE THE SYSTEM TIME AND TIME ZONE.....	87
7.2.3	CONFIGURE THE LOGIN WELCOME MESSAGE.....	87
7.2.4	CONFIGURE THE SYSTEM EXCEPTION PROCESSING MODE. ....	88
7.2.5	CONFIGURE TO RESTART THE DEVICE. ....	89
7.2.6	CONFIGURE THE HISTORY COMMAND SAVING FUNCTION. ....	90
7.2.7	CONFIGURE THE LOGIN SECURITY SERVICE. ....	91
7.2.8	CONFIGURE CPU MONITORING.....	92
7.2.9	CONFIGURE DISPLAY OF PROPERTIES IN PAGES. ....	93
7.2.10	OPERATION RECORD FILE MANAGEMENT .....	94
7.2.11	CONFIGURE SYSTEM SECURITY MODE. ....	94
7.2.12	SYSTEM MANAGING, MONITORING, AND MAINTAINING.....	94
7.2.13	CONFIGURE THE FLEXIBLE TABLE ENTRY MODE. ....	96
<b>7.3</b>	<b>TYPICAL CONFIGURATION EXAMPLE OF SYSTEM MANAGEMENT .....</b>	<b>97</b>
7.3.1	CONFIGURE USER- AND IP-BASED LOGIN RESTRICTIONS.....	97
7.3.2	CONFIGURE QUICK LOGIN RESTRICTIONS .....	99
<b>8</b>	<b>SYSTEM ALARM .....</b>	<b>101</b>
<b>8.1</b>	<b>OVERVIEW .....</b>	<b>101</b>
<b>8.2</b>	<b>SYSTEM ALARM FUNCTION CONFIGURATION.....</b>	<b>101</b>
8.2.1	CONFIGURE SYSTEM TEMPERATURE ALARMS .....	101
8.2.2	CONFIGURE SYSTEM CPU ALARMS .....	102



8.2.3	CONFIGURE THE LOW THRESHOLD OF MEMORY USAGE.....	103
8.2.4	CONFIGURE SYSTEM MEMORY ALARMS .....	103
8.2.5	CONFIGURE SYSTEM POWER SUPPLY ALARMS.....	104
8.2.6	CONFIGURE SYSTEM FAN ALARMS .....	104
<b>9</b>	<b>SYSTEM LOG CONFIGURATION .....</b>	<b>105</b>
<b>9.1</b>	<b>OVERVIEW .....</b>	<b>105</b>
<b>9.2</b>	<b>SYSTEM LOG FUNCTION CONFIGURATION.....</b>	<b>106</b>
9.2.1	CONFIGURE LOG OUTPUT FUNCTIONS .....	107
9.2.2	CONFIGURE THE TIMESTAMP FOR LOGS .....	112
9.2.3	CONFIGURE OPERATION LOG OUTPUT TO THE LOG HOST.....	112
9.2.4	CONFIGURE LOG SUPPRESSION .....	113
9.2.5	CONFIGURE LOG FILES CAPACITY .....	114
9.2.6	CONFIGURE LOG FILES ENCRYPTION.....	114
9.2.7	CONFIGURE LOG DISPLAY COLOR.....	115
9.2.8	CONFIGURE LOG FILTERING FUNCTION .....	116
9.2.9	CONFIGURE THE ORIGIN-ID OF A DEVICE .....	116
9.2.10	LOG MONITORING AND MAINTAINING .....	117
<b>10</b>	<b>SOFTWARE UPGRADE.....</b>	<b>118</b>
<b>10.1</b>	<b>OVERVIEW .....</b>	<b>118</b>
<b>10.2</b>	<b>SOFTWARE UPGRADE FUNCTION CONFIGURATION.....</b>	<b>120</b>
10.2.1	UPGRADE THE IMAGE PROGRAM PACKAGE.....	120
10.2.2	PATCH PROGRAM UPGRADE. ....	122
10.2.3	BOOTLOADER PROGRAM UPGRADE .....	123
10.2.4	DEVINFO FILE UPGRADE .....	127
10.2.5	PACKAGE FILE UPGRADE .....	129
<b>10.3</b>	<b>EXAMPLE OF TYPICAL CONFIGURATION FOR SOFTWARE UPGRADE .....</b>	<b>131</b>
10.3.1	UPGRADE PACKAGE FILE.....	131
10.3.2	FULL UPGRADE OF ALL SOFTWARE VERSIONS.....	133
10.3.3	UPGRADE BOOTLOADER USING CONSOLE PORT. ....	137
<b>11</b>	<b>BOOTLOADER .....</b>	<b>140</b>

<b>11.1</b>	<b>OVERVIEW .....</b>	<b>140</b>
<b>11.2</b>	<b>BOOTLOADER FUNCTION CONFIGURATION.....</b>	<b>140</b>
11.2.1	PREPARATION FOR BOOTLOADER FUNCTION CONFIGURATION .....	141
11.2.2	ENTER THE BOOTLOADER CONFIGURATION MODE.....	141
11.2.3	SET BOOTLOADER STARTUP PARAMETERS .....	142
11.2.4	UPGRADE BOOTLOADER PROGRAM. ....	143
11.2.5	BOOTLOADER MONITORING AND MAINTAINING.....	144
<b>11.3</b>	<b>BOOTLOADER TYPICAL CONFIGURATION EXAMPLE .....</b>	<b>144</b>
11.3.1	CONFIGURE THE BOOTLOADER TO START THE IMAGE PROGRAM VIA THE NETWORK. ....	144
<b>12</b>	<b>POE MANAGEMENT .....</b>	<b>145</b>
<b>12.1</b>	<b>OVERVIEW .....</b>	<b>145</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>146</b>
<b>12.1.2</b>	<b>POE POWER SUPPLY PROCESS .....</b>	<b>147</b>
<b>12.2</b>	<b>POE FUNCTION CONFIGURATION .....</b>	<b>148</b>
<b>12.2.1</b>	<b>POE BASIC FUNCTION CONFIGURATION .....</b>	<b>149</b>
<b>12.2.2</b>	<b>CONFIGURE THE POE POWER .....</b>	<b>151</b>
<b>12.2.3</b>	<b>CONFIGURE POWER SUPPLY PRIORITIES .....</b>	<b>153</b>
<b>12.2.4</b>	<b>CONFIGURE PD POWER-UP AND POWER-DOWN PARAMETERS .....</b>	<b>155</b>
<b>12.2.5</b>	<b>CONFIGURE THE ABNORMALITY RECOVERY FUNCTION .....</b>	<b>158</b>
<b>12.2.6</b>	<b>CONFIGURE POE POWER ALARM THRESHOLD .....</b>	<b>159</b>
<b>12.2.7</b>	<b>POE MONITORING AND MAINTAINING .....</b>	<b>160</b>
<b>13</b>	<b>PDI .....</b>	<b>160</b>
<b>13.1</b>	<b>OVERVIEW .....</b>	<b>160</b>
<b>13.2</b>	<b>CONFIGURE PDI BASIC FUNCTIONS .....</b>	<b>160</b>
<b>13.3</b>	<b>CONFIGURE THE ARP MESSAGE DELIVERY INTERVAL. ....</b>	<b>160</b>
<b>13.4</b>	<b>CONFIGURE THE NUMBER OF RETRIES FOR ARP MESSAGE DELIVERY. ....</b>	<b>161</b>
<b>13.5</b>	<b>CONFIGURING IP INSPECTION TABLE ENTRIES.....</b>	<b>161</b>
<b>13.6</b>	<b>PDI MONITORING AND MAINTAINING .....</b>	<b>161</b>
<b>14</b>	<b>LUM.....</b>	<b>162</b>
<b>14.1</b>	<b>OVERVIEW .....</b>	<b>162</b>

<b>14.2 LUM FUNCTION CONFIGURATION.....</b>	<b>163</b>
14.2.1 CONFIGURE ACCESS .....	163
14.2.2 CONFIGURE LOCAL USERS.....	165
14.2.3 CONFIGURE ADMINISTRATOR USER ATTRIBUTES.....	166
14.2.4 CONFIGURE ACCESS USER ATTRIBUTES.....	169
14.2.5 CONFIGURE LOCAL USER GROUPS.....	169
14.2.6 CONFIGURE PASSWORD POLICIES.....	171
14.2.7 LUM MONITORING AND MAINTAINING.....	174
<b>14.3 TYPICAL LUM CONFIGURATION EXAMPLE .....</b>	<b>174</b>
14.3.1 CONFIGURE NETWORK ADMINISTRATOR USERS .....	174
<b>15 ZTP.....</b>	<b>175</b>
<b>15.1 OVERVIEW .....</b>	<b>175</b>
<b>15.2 ZTP FUNCTION CONFIGURATION .....</b>	<b>177</b>
15.2.1 ENABLE OR DISABLE ZTP FUNCTION.....	177
15.2.2 ZTP MONITORING AND MAINTAINING .....	178
<b>15.3 ZTP TYPICAL CONFIGURATION EXAMPLE.....</b>	<b>178</b>
15.3.1 CONFIGURE ZTP TO USE COMMON INTERMEDIATE FILES FOR ZERO-CONFIGURATION DEPLOYMENT VIA DHCP .....	178
15.3.2 CONFIGURE ZTP TO USE PYTHON INTERMEDIATE FILES FOR ZERO-CONFIGURATION DEPLOYMENT VIA DHCP .....	181
15.3.3 CONFIGURE ZTP TO USE COMMON INTERMEDIATE FILES FOR ZERO-CONFIGURATION DEPLOYMENT VIA USB.....	185
15.3.4 CONFIGURE ZTP TO USE PYTHON INTERMEDIATE FILES FOR ZERO-CONFIGURATION DEPLOYMENT VIA USB.....	188
15.3.5 CONFIGURE ZTP TO AUTOMATICALLY COMPLETE STACKING USING PYTHON INTERMEDIATE FILES VIA DHCP .....	190

# 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. · Display the system information
Privileged user mode	In common user mode, run the	Hostname#	Run the <b>disable</b> or <b>exit</b> command to exit to the	· Configure the operating parameters of the device

Mode	How to Enter the Mode	System Prompt	How to Exit the Mode	Functions
	<b>enable</b> command.		common user mode.	· Display the operating information of the device
Global configuration mode	In privileged user mode, run the <b>configure terminal</b> 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 mode	In global configuration mode, run the <b>ip access-list standard</b> or <b>ip access-list extended</b> command.	Hostname(config-std-nacl)# Hostname(config-ext-nacl)#	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.	Configures the Access Control List (ACL). The configuration tasks include:  · 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	The inputted command is incomplete.



Error Message	Error Cause
or % Incomplete command	
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+N 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.
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.
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.

# 2System 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.
	The device acts as an SSH client for remote login.
Configure remote login through WEB.	Configure remote login through HTTP.

## Configuration Task

Configure remote login through HTTPS.



Note:

- For the related user configuration of Telnet and SSH remote login, refer to the section on "Login Control and Management" in the User Manual.

### 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

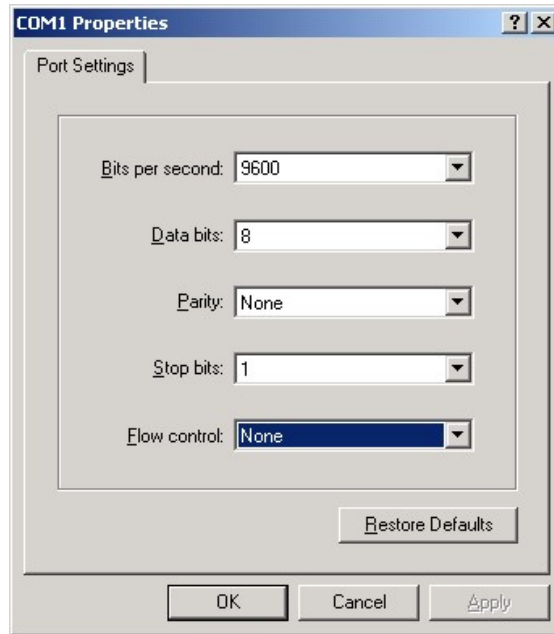


Figure 2-4 Configuring Parameters for the Serial Communication Port

- 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>	-

Step	Command	Description
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 interface-name</b> ] <i>user auth-method 1 password</i>	Mandatory



Note:

- 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 Remote 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

Step	Command	Description
		By default, the WEB server is not enabled.
Configure the HTTP server port.	<b>ip http port</b> <i>port_number</i>	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 Remote 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.
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.

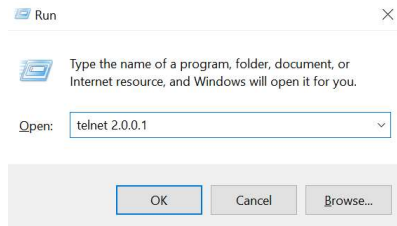


Figure 2-6 Telnet to the Device on PC

Step 5: Check the result.

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

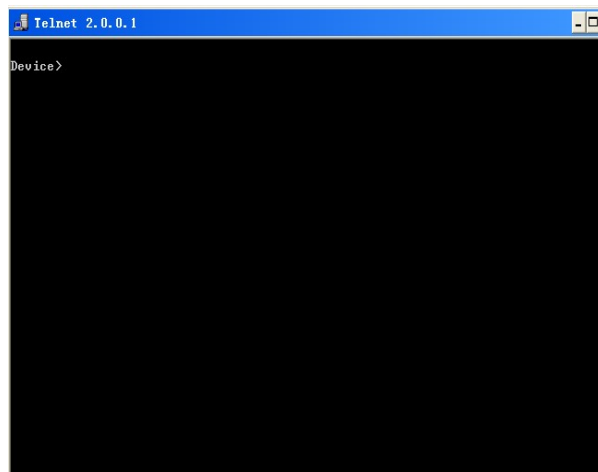


Figure 2-7 Window Displayed after Telnet Success

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

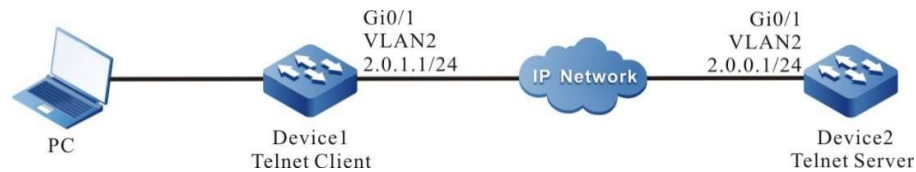


Figure 2-8 Network Topology for Configuring a Local Device to Telnet to a Remote Device

#### 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

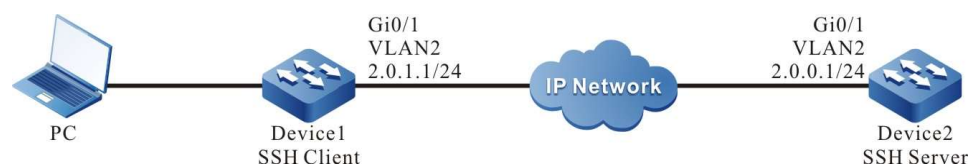


Figure 2-9 Network Topology for Configuring a Local Device to Log in to a Remote Device via SSH

#### 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
```

### 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.



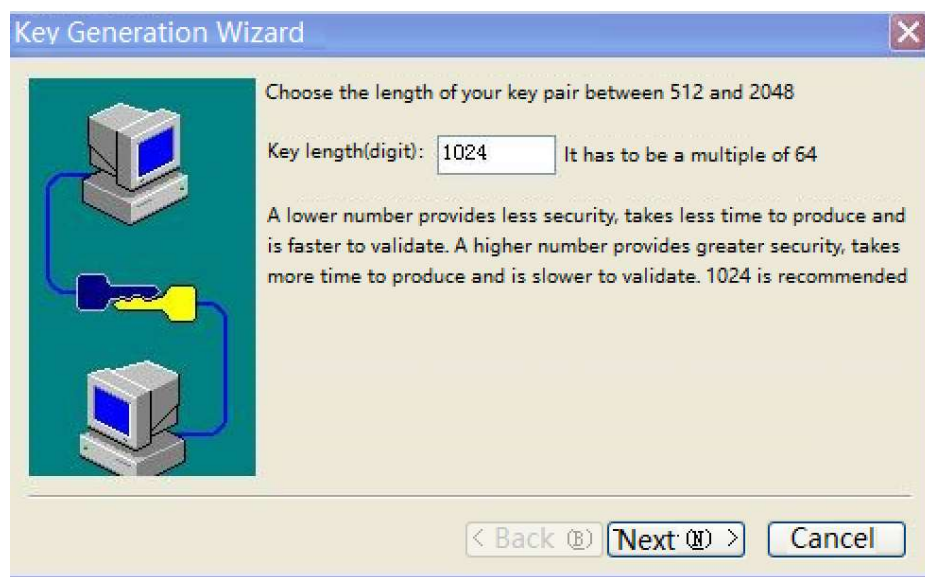
# Key type, choose either from DSA and RSA, here DSA is chosen as an example, click on Next.



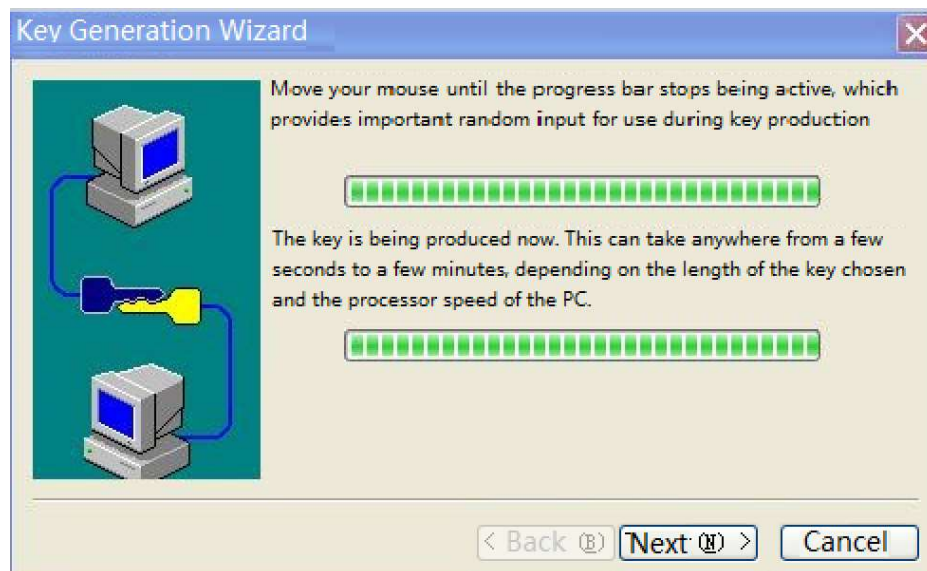
#Passphrase is locally valid and can be ignored, click on Next.



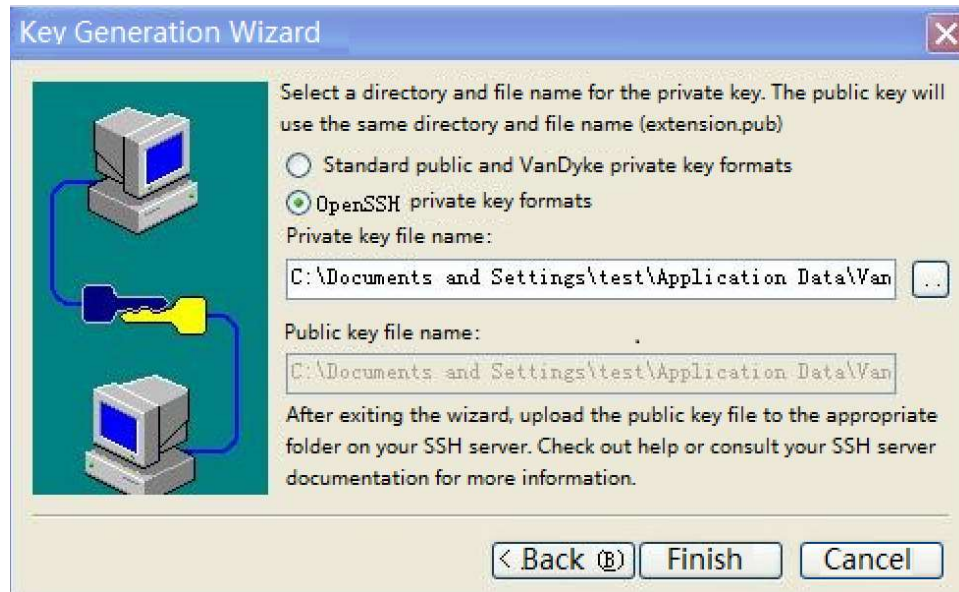
\#Key length to be filled in according to the instructions, click on Next.



#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
```



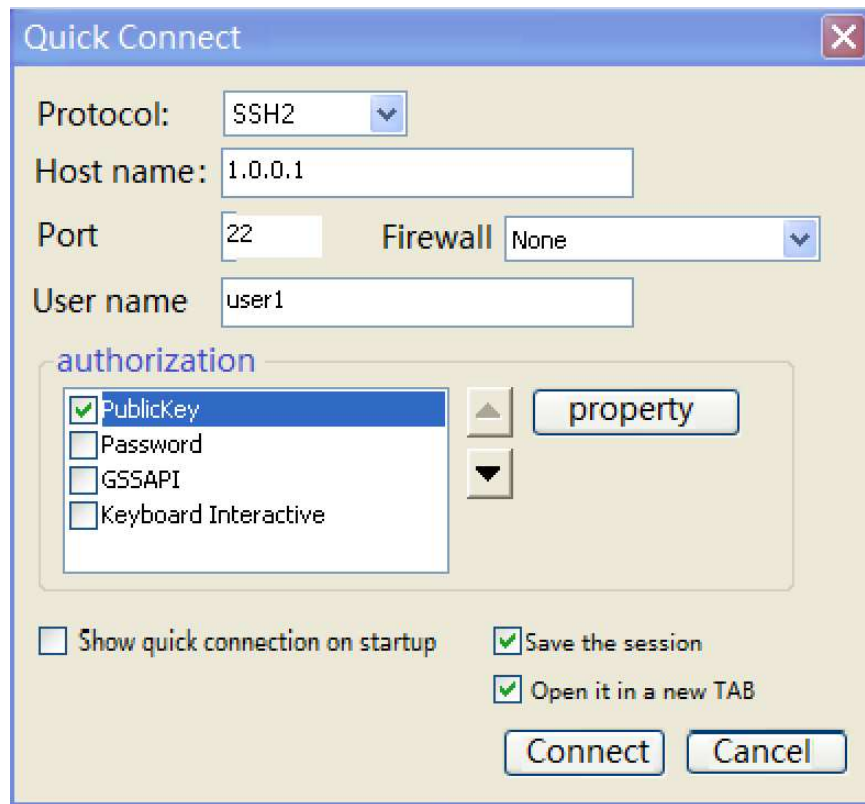
Note:

- 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.



The image shows a "Quick Connect" dialog box with a blue title bar and a close button (X) in the top right corner. The dialog contains the following fields and options:

- Protocol:** A dropdown menu showing "SSH2".
- Host name:** A text input field containing "1.0.0.1".
- Port:** A text input field containing "22".
- Firewall:** A dropdown menu showing "None".
- User name:** A text input field containing "user1".
- authorization:** A section with a list box containing four items: "PublicKey" (checked), "Password", "GSSAPI", and "Keyboard Interactive". To the right of the list box are up and down arrow buttons and a "property" button.
- Checkboxes:** At the bottom, there are four checkboxes: "Show quick connection on startup" (unchecked), "Save the session" (checked), "Open it in a new TAB" (checked), and "Show quick connection on startup" (unchecked).
- Buttons:** At the bottom right, there are two buttons: "Connect" and "Cancel".



# 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, \$enab+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 \$enab10\$. 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.
-

### Configuration Condition

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> [ <i>level 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>	-
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</b> { <b>con 0</b>   <b>vtty</b> <i>vtty-min-number</i> [ <i>vtty-max-number</i> ] }	Mandatory
Configure the commands to be automatically executed after successful login.	<b>autocommand</b> <i>command-line</i>	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</b> { <b>con 0</b>   <b>vtty</b> <i>vtty-min-number</i> [ <i>vtty-max-number</i> ] }	Mandatory
Configure the auto command execution options.	<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> ] }	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</b> { <b>con 0</b>   <b>vtty</b> <i>vtty-min-number</i> [ <i>vtty-max-number</i> ] }	Mandatory
Configuring the idle timeout exit time.	<b>exec-timeout</b> <i>exec-timeout-minute_number</i> [ <i>exec-timeout-second_number</i> ]	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</b> { <b>con 0</b>   <b>vtty</b> <i>vtty-min-number</i> [ <i>vtty-max-number</i> ] }	Mandatory
Configure the line password.	<b>password 0</b> <i>password</i>	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</b> { <b>con 0</b>   <b>vtty</b> <i>vtty-min-number</i> [ <i>vtty-max-number</i> ] }	Mandatory
Configure the login authentication mode.	<b>login</b> { <b>aaa</b> [ <i>domain-name</i>   <b>default</b> ]   <b>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</b> { <b>con 0</b>   <b>vtty</b> <i>vtty-min-number</i> [ <i>vtty-max-number</i> ] }	Mandatory
Configure the timeout time for user login.	<b>timeout login respond</b> <i>respond-time-value</i>	Mandatory By default, the time to enter the username or password before the session timeout is 30

Step	Command	Description
		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 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>	-
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

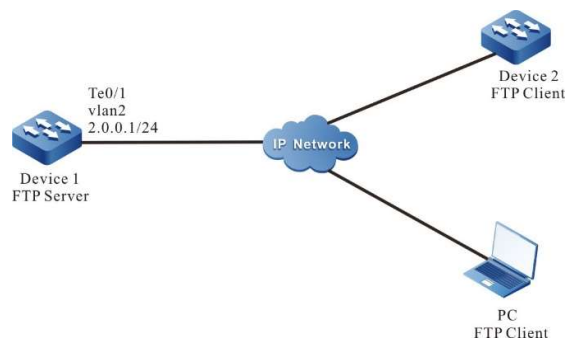


Figure4-2 Network Topology in Which a Device Acts as an FTP Server

## 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>
```

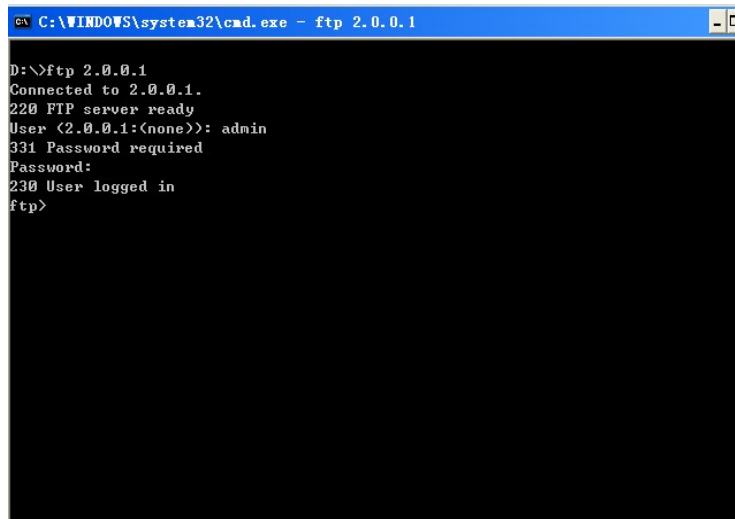
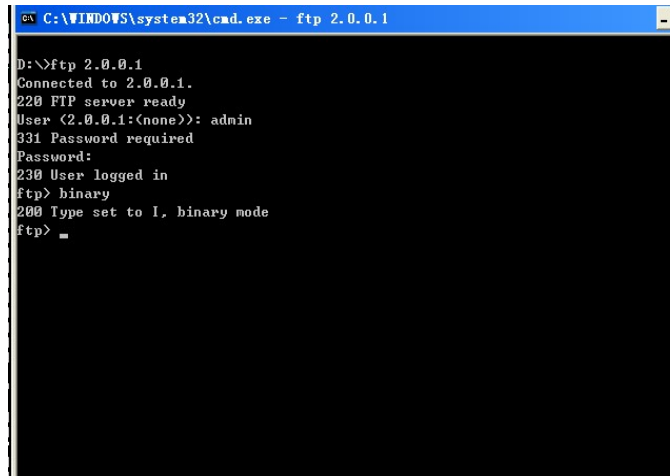


Figure 4–3 Logging in to the FTP server from the DOS interface

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

ftp>binary



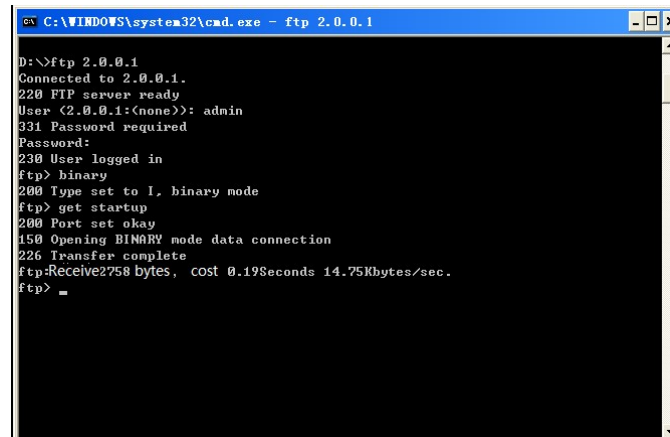
```
C:\WINDOWS\system32\cmd.exe - ftp 2.0.0.1

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 0.19Seconds 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
```



Note:

- 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.

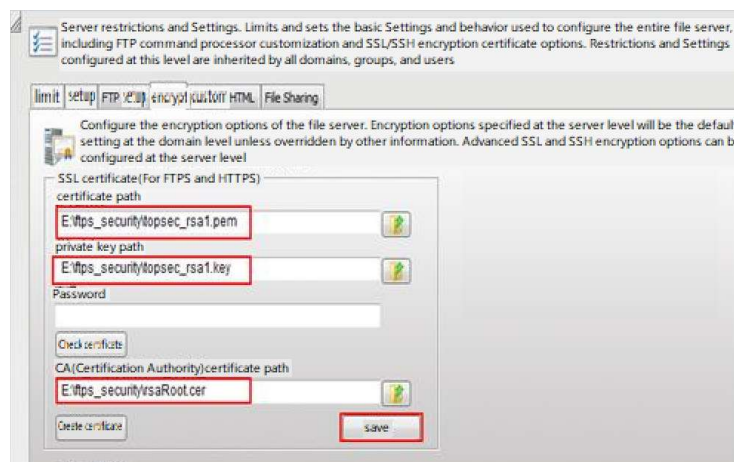
#### Network Topology



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
% Input the certificate data, press <Enter> twice to finish:
-----BEGIN CERTIFICATE-----
MIIDBzCCAnCgAwIBAgITpXH17Hj/AswDQYJKoZIhvcNAQEFBQAwYjELMAkGA1UE
BhMCQ04xEDAOBgNVBAgMB0JFSUpJTkcxDjAMBGNVBAoMBUNJRUNDMDQ8wDQYDVQQL
DAZHHRkEgQ0ExIDAeBgNVBAMMF01pbmldQSBGcmVCU0QgUm9vdCBDZXJ0MB4XDTA5
MDgwMzA2MDY1MloXDTE5MDgwMzA2MDY1MlowYjELMAkGA1UEBhMCQ04xEDAOBgNV
BhMCQ0JFSUpJTkcxDjAMBGNVBAoMBUNJRUNDMDQ8wDQYDVQQLDAZHHRkEgQ0ExIDAe
BgNVBAMMF01pbmldQSBGcmVCU0QgUm9vdCBDZXJ0MIGeMA0GCSqGSIb3DQEBAQUA
A4GMADCBiAKBgHXZMtpxzH8p0uUt6QomUhuJNcy9iyYhoJVx4I3T6kpmx9cdzapM
RoKUa9eB/jCzhgctQc7ZDuKP+gafHWgZtbzwwSVksVsNmFqBivixveGx9dCrtequ
+vDiXVYdVPSNDDTmamMGYyCb0N7aSOzdgV6BYyQKyy/Y0FK6/v/v4NUxAgMBAAGj
gcYwgcMwPQYDVR0fBDYwNDAyoDCgLoYsaHR0cDovLzE2OC4xNjguMTcuNDY6OTAw
MC9nZmEvY3JsL2dmYWwFwcC5jcmwwSAyDVR0gBEewPzA9BggrBgEEAYcrMjAxMC8G
CCsGAQUFBwIBFiNodHRwOi8vd3d3LmdmYXBraS5jb20uY24vcG9saWN5LmRvYzAL
BgNVHQ8EBAMCAuQwDAYDVR0TBAAUwAwEB/zAdBgNVHQ4EFgQUhnY8uZXbE2iX1mXO
ipvfUDUgAeswDQYJKoZIhvcNAQEFBQADgYEAeNPdTE+YpfOQn8IW1oF7TkGJ/Vzd
c0O5UUB+PhYkj+FXUX8WyxabOxgl3u+7DJ/3gHw1rO8ZcDO94Wz+nBsile5tFv7
/bHz0yqJVoUJMIaWODmLXJ5f15GeBCprzLM88RJCv6LBHfg4ThOC4Ds80Ssive1
eAod+7kbmVPOZg8=
-----END CERTIFICATE-----
```

% Input the private key data, press <Enter> twice after data to finish or press <Enter> without data to ignore:

% The Root CA Certificate has the following attributes:

```
Serial Number: 4e95c7d7b1e3fc0b
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
Usage: General
```

Fingerprint(sm3):18d39e4c50c9ad8b11446ac7ac1736f853ac92e769994b98233b48787562429c  
Fingerprint(sha1):ab3559e26384539ffac3c76b5a5e7a1f7073dfb

% Do you accept this root ca-certificate[yes]/[no]:  
% Please answer 'yes' or 'no'.  
% Do you accept this root ca-certificate[yes]/[no]:

Nov 11 2015 19:06:04: %PKI-CERTIFICATE\_STATECHG-5: Certificate(issuer:C=CN, ST=BEIJING, O=CIECC, OU=GFA CA, CN=MiniCA FreeBSD Root Cert, sn:4E95C7D7B1E3FC0B, subject:C=CN, ST=BEIJING, O=CIECC, OU=GFA CA, CN=MiniCA FreeBSD Root Cert) state valid  
% PKI: Import Certificate success.

#Open the user certificate (topsec\_rsa2\_myself.pem) and the private key certificate (topsec\_rsa2\_myself.key) with Notepad, then copy the content inside, enter the command crypto ca import certificate to test in shell, and follow the prompts to import the certificates in order into the device domain test:

```
Device(config)#crypto ca import certificate to test
% Input the certificate data, press <Enter> twice to finish:
-----BEGIN CERTIFICATE-----
MIIDVTCCAr6AwIAgIQEJ7twbl3pDlZj99DFOKOzANBgkqhkiG9w0BAQUFADBIMQswCQYDVQQGEwJDTjEQMA
4GA1UECAwHQkVJSklORzEOMAwGA1UECgwFQ0lFQ0MxMzANBgNVBAsMBkdGQSBDDQTEgMB4GA1UEAwwXTW
luaUNBIEZyZyUJTRCBSb290IENlcnQwHhcNMTIwNjI2MDUwMTIzWjBjMQswCQYDVQQGEwJDTjEQMA
4GA1UECAwHYmVpamluZzESMBAGA1UEBwwJZG9uZ2NoZW5nMQ4wDAYDVQQKDAVjaVWVjYzE
MMAoGA1UECwwDZ2ZMR0wGwYJKoZIhvcNAQkBFg50ZXN0QGVjLmNvbS5jbjENMAsGA1UEAwwEcnNhMjCBnz
ANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA6A1NqTnNsV9Yyij2tTMppB9C5VCLtkPh9KIIq/ZTIVhrJED+N5HVfQQy
ZYS/z4JWAip50dyP1+NP+bvP+pb9CfEaJ8+ObYQnfUH6qiPccLkWO3XYanu6Dw5EMJYntwglSKmk1Pcc+j+yzWnwYMD
FcbSsQ+8J5UzlesFhU7GnXacAwEAAaOB7jCB6zA+BgNVHR8ENZAlMDOgMaAvhi1odHRwczovLzIxMS44OC4yNS4x
ODo4NDQ0L2dmYS9jcmwvUINBMTAyNC5jcmwvUQYDVROgBEowSDBGBggrBgEEAYcrMjA6MDgGCCsGAQUFBwI
BFixodHRwczovLzIxMS44OC4yNS4xODo4NDQ0L2dmYS9jcmwvUINBMTAyNC5wbDALBgNVHQ8EBAMCA/gwCQY
DVR0TBAlwADAdBgNVHQ4EFgUUp/9/ODGLR84syxPaBkLG3mCpU5YwHwYDVROjBBgwFoAUhnY8uZXbE2iX1mX
OipvfUdUGAeswDQYJKoZIhvcNAQEFBQADgYEAYrFZQrNHoLn9odeGctzTRGVmMcv9sJ0ncgUEfbrLu6QUodQy3jix
WFIxheJK1btff66/ShuKtZpqJ1WE9I92tflHwLpXT0gujtxNi02TOPBNEU7P9nUgxfDG+uhyPTeufSkfn3LCTHmGfVORF2s
oGSLaUPV1Zy5E9hmFZoMhs=
-----END CERTIFICATE-----
```

```
% Input the private key data, press <Enter> twice after data to finish or press <Enter> without data to ignore:
-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQDoCU2pOc2xX1jKKPa1MymkH0LIU2Q+H0qUir9IOVWGskQP43kdV9BDJhL/PglYCKnnR3I/X40/
5u8/6lv0J8RonZ45thCd9Qfqql9xwuRY7ddhqe7oPdkQwlie3CCVlqaTU9xz6P7LNaftBgwMVxtKx7wnlTOV6wWFTsaddpw
IDAQABAoGBAMnJNWliJfG4+1CvHGN4buhmApWBnnmBL1A7jrlh4CMGPi5MJrgzvjeSnlwfWIXJXbSu4feuJT1UFqMk
uyIm9l+k8Rm3hjCIXlIFNV/ykG6a6GIVFYGxQWwL50Pm6S7xXL9Ryd6hnOHUUtwwLvkpBTx/4qvrIABDtxRjVglvApAk
EA9BN1Zxm31BOyeB6KXvwmXD6/+dGaDfE4Dbcijy1LgKliaEBJ00e/0R9ekg6myGTU2asJvPtkaXPqcvwU6+e2mwJBAPN
fRtk9LzUlnmTV2DrsE9k3rbPnqQs9wb/mLUNdv2FQeoY/Zf4qh0WXsug2q/6GPsvLUA7mbdArGFUwwQbw3+UCQQC8r2
5LSogX40JM6g8+bq4fEcOHdSoLLTeQlstdC9yP3/75/cqhoUbPYz2jK0SriB+RWM53X46pDn4b8P2RAKBGjoBLL+nXx
ooWgcjGjFrUxsedOLTIPhtFvz2wfiWx2NsswISZQ0skae58VB1ZFSJvguoa58M+bsAHMrNDh+HhAkBcNAjKBDdVw0ll6bN
oRGugEvuo3Z3O0kbVcjZld+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: 4e95c7d7b1e3fc0b
  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):504599a2f170c51b62b2f8b0850f33a5595bc9e592d14eac9c90b1e59de35a89
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>	-



Step	Command	Description
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>	-

Step	Command	Description
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>	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>	-

Step	Command	Description
Copy a file.	<b>copy</b> <i>src-parameter dest-parameter</i>	Mandatory



Note:

- The copy command can be used to copy file between the file system, the FTP server, and the TFTP server. For details, refers to the section on copy command in the User 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</b> <i>path/filename</i>	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>	-
Download a File from the FTP Server	<b>{ftpcopy   ftpscopy} [ vrf vrf-name ] host-ip-address username password src-filename { /flash   /syslog   usb   dest-filename }</b>	Optional



Note:

- The ftpcopy command can be used to download the file from the FTP server to the file system. For details about the operation, refer to the section on ftpcopy command and ftpscopy command in the User 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>	-
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</b> <b>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	<b>copy startup-config { file-system dest-filename   ftp</b>	Mandatory

Step	Command	Description
host through the FTP protocol.	<pre>[ vrf vrf-name ] { hostname   ip-address } username password dest-filename   <b>ftps</b> [ vrf vrf-name ] { hostname   ip-address } username password dest-filename <b>VerifyType</b> { none   peer }  <b>tftp</b> [ vrf vrf-name ] { hostname   ip-address } dest-filename }</pre>	

### 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.	<pre><b>copy</b> { <b>file-system</b> src-filename   <b>ftp</b> [ vrf vrf-name ] { hostname   ip-address } username password src-filename   <b>ftps</b> [ vrf vrf- name ] { hostname   ip-address } username password src-filename   <b>tftp</b> [ vrf vrf-name ] { hostname   ip-address } src- filename } { <b>file-system</b> dest- filename   <b>startup-config</b> }</pre>	Mandatory



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</b> <i>vrf-name</i> ] { <i>hostname</i>   <i>ip-address</i> } <i>user-name</i> <i>password file-name</i> } }   <b>ftps</b> [ <b>vrf</b> <i>vrf-name</i> ] { <i>hostname</i>   <i>ip-address</i> } <i>user-name</i> <i>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> [ <i>context</i> ] } <i>expression</i>   <b>redirect</b> { <b>file</b> <i>filename</i>   <b>ftp</b> [ <b>vrf</b> <i>vrf-name</i> ] { <i>hostname</i>   <i>ip-address</i> } <i>user-name</i> <i>password file-name</i> } }   <b>ftps</b> [ <b>vrf</b> <i>vrf-name</i> ] { <i>hostname</i>   <i>ip-address</i> } <i>user-name</i> <i>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.
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

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the system time.	<b>clock timezone</b> <i>timezone-name-string hour-offset-number</i> [ <i>minute -offset-number</i> ]	Mandatory  The default is Universal Time Coordinated (UTC).
Enter the privileged user mode.	<b>exit</b>	-
Configure the system time.	<b>clock</b> <i>year-number</i> [ <i>month-number</i> [ <i>day-number</i> [ <i>hour-number</i> [ <i>minute-number</i> [ <i>second-number</i> ] ] ] ] ]	Mandatory

## 7.2.3 Configure the login welcome message.

### Configuration Condition

None

#### Configure the login welcome message.

When a user logs in to the device for login authentication, the login welcome message is displayed. The welcome message can be configured according to the requirement.

Table 7-4 Configuring the Login Welcome Message

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure the login welcome message.	<b>banner motd</b> <i>banner-line</i>	Mandatory

### 7.2.4 Configure the system exception processing mode.

#### Configuration Condition

None

#### Configure the system exception processing mode.

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



Step	Command	Description
		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 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 { telnet   ssh   ftp   snmp }</b>	Mandatory  By default, the system login

Step	Command	Description
		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 telnet ip-addr 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 telnet ip-addr 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 address from recording information.	<b>login-secure telnet ip-addr record-aging-time</b> <i>record-aging-time-number</i>	Mandatory By default, the aging time is 15 minutes.

## 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</i>   <i>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</i> <i>password</i> <i>file-name</i>   <b>ftps</b> [ <b>vrf</b> <i>vrf-name</i> ] { <i>hostname</i>   <i>ip-address</i> } <i>user-name</i> <i>password</i> <i>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.
<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>pended</b>   <b>unpended</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

Command	Description
	system.
<b>show system fan [brief]</b>	Display system fan information.
<b>show system lpu [ lpu-num   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 [brief mpu-num ]</b>	Display system MPU information.
<b>show system power [ power-num   brief ]</b>	Display system power information.
<b>show tech-support { sys-base [ detail ]   drv-base [ detail ]   l2-base [ detail ]   l3-base [ detail ]   all } [ page   to-memory   to-flash ]</b>	Display technical support information.
<b>show version [ 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

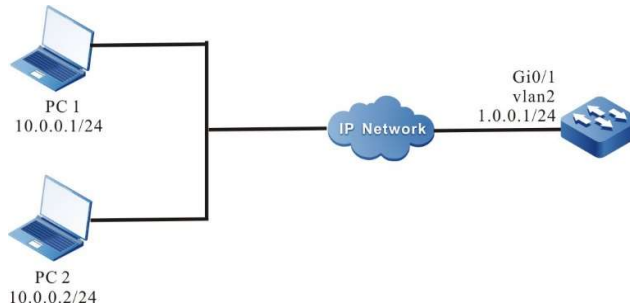


Figure 7-1 Network Topology for Configuring User- and IP-based Login Restrictions

#### 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
```

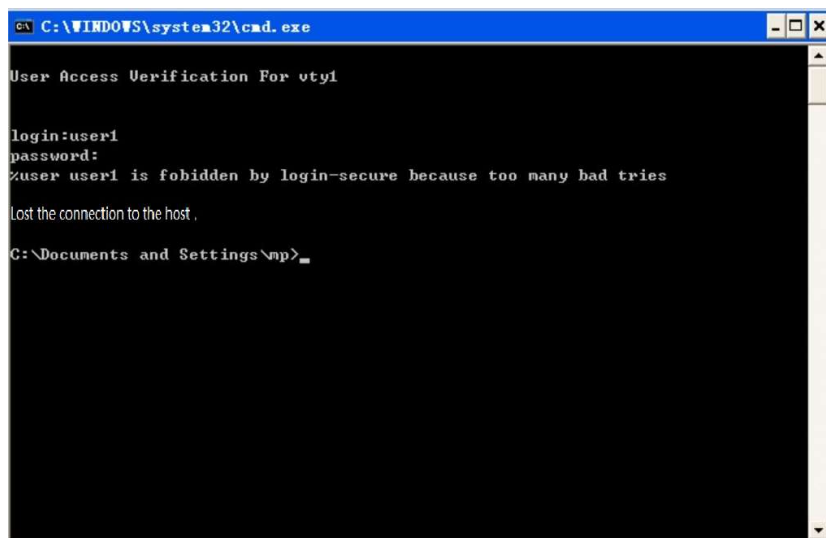
Step 4: Check the result.

#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

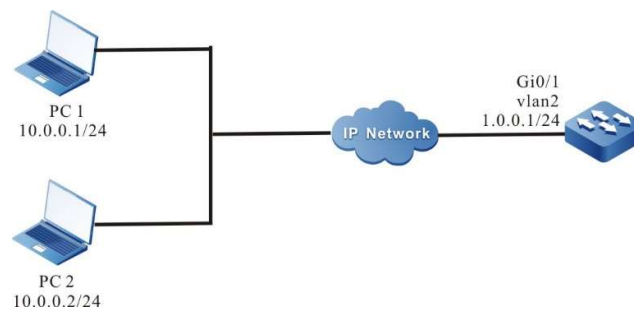


Figure 2-7 Network Topology for Configuring Quick Login Restriction

#### 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</b><br><b>{ switch   cpu } 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</b><br><b>device-num mpu { switch </b><br><b>cpu } 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             | <b>cpu utilization warner-</b> | Optional    |

| Step                        | Command                                | Description |
|-----------------------------|----------------------------------------|-------------|
| utilization alarm threshold | <b>threshold</b> [ <i>rate-value</i> ] |             |

### 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</b> <i>low-value</i> | Optional<br>By default, the low threshold of system memory is 32M. |

### 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 warn-<br/>threshold [ <i>rate-value</i> ]</b> | Optional<br><br>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 7 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.<br>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.<br><br>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.<br>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          |

| Configuration Task                               |                                                  |
|--------------------------------------------------|--------------------------------------------------|
|                                                  | 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<br>By default, the log output |

| Step                                       | Command                                                                                                                        | Description                                                            |
|--------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------|
|                                            |                                                                                                                                | function is enabled.                                                   |
| Enable log display on the control console. | <b>logging source</b> { <i>module-name</i>   <b>default</b> } <b>console</b><br>{ <b>level</b> <i>severity</i>   <b>deny</b> } | Optional<br>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<br>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><br>{ <b>level</b> <i>severity</i>   <b>deny</b> } | Optional<br>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<br>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> | -           |

| Step                                                        | Command                                                                                                                                                                                                                                                                                      | Description                                                                                                                                                                                                                      |
|-------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Enable the log output function.                             | <b>logging enable</b>                                                                                                                                                                                                                                                                        | Optional<br>By default, the log output function is enabled.                                                                                                                                                                      |
| Configure Log Output to the Log Server                      | <b>logging server</b> <i>server-name</i><br>[ <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> }<br>[ <b>port</b> <i>port-num</i> ] [ <b>facility</b> <i>facility-name</i> ] [ <b>level</b> <i>severity</i> ] | Mandatory<br>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<br>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<br>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<br>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<br>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<br>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<br>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><br><b>logging compress max-num value</b>      | Optional<br>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<br>By default, the log output function is enabled. |

| Step                                                                               | Command                                            | Description                                                                                                                         |
|------------------------------------------------------------------------------------|----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| Configure Email Template                                                           | <b>logging email</b> <i>email-profile</i>          | Mandatory<br>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<br>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<br>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<br>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<br>By default, no email password of the sender of the log information is configured.                                      |
| Configure the email domain address of the recipient receiving the log information. | <b>mail server</b> <i>server-name</i>              | Optional<br>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<br>By default, no email subject of the sender of the log information is configured.                                        |
| Configure a specified level of log                                                 | <b>logging source</b> { <i>module-</i>             | Optional                                                                                                                            |

| Step                                                                                            | Command                                                                                | Description                                           |
|-------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|-------------------------------------------------------|
| information to be outputted to the corresponding recipient and copy-to email address via email. | <i>name</i>   <b>default</b> } <b>email</b><br>{ <i>level severity</i>   <b>deny</b> } | 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<br>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<br>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<br>By default, the log output function is enabled.                                       |
| Configure Log Host                               | <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<br>By default, the function of sending logs to the log server is not enabled.           |
| Configure operation log output to the log server | <b>logging operation to-server</b>                                                                                                                                                                                                                                                     | Mandatory<br>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 | <b>configure terminal</b> | -           |

| Step                                                 | Command                                                            | Description                                                              |
|------------------------------------------------------|--------------------------------------------------------------------|--------------------------------------------------------------------------|
| configuration mode.                                  |                                                                    |                                                                          |
| Configure the function of log duplicate suppression. | <b>logging suppress duplicates interval</b><br><i>interval-num</i> | Mandatory<br><br>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<br><br>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       | <i>logging file encryption</i><br><i>algorithm SMV4 key</i><br><i>password</i> | Optional<br>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 logging-color</i> ] | Optional<br>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<br>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 9-17 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><br><i>origin-id</i> | Optional<br>By default, the origin-id of a device is not configured. |

## 9.2.10 Log Monitoring and Maintaining

Table 9-18 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 Ymodem 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.
- **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<br>Package | fpga<br>Procedures | bootloader<br>Procedures | cpld<br>Procedures | devinfo<br>DOCUMENTATION | patch<br>DOCUMENTATION | package<br>Package file |
|----------------------------|------------------|--------------------|--------------------------|--------------------|--------------------------|------------------------|-------------------------|
| Main Processing Unit (MPU) | √                | √                  | √                        | √                  | √                        | √                      | √                       |



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

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

```
Hostname#sysupdate image mpu 130.255.168.45 sp7-g-9.7.1.1(74)(R).pck ftp a a
```

#The device will prompt the following:

```
checking "sp7-g-9.7.1.1(74)(R).pck" : ...OK
The file sp7-g-9.7.1.1(74)(R).pck already exists on Mpu 0, overwrite it?(Yes|No):y
downloading "sp7-g-9.7.1.1(74)(R).pck" :
#####OK
Download "sp7-g-9.7.1.1(74)(R).pck" (95678892 Bytes) successfully.
Verify the image...
Apr 16 2021 03:11:33 BCM_hezi-ss69 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 03:12:08 BCM_hezi-ss69 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 03:12:28 BCM_hezi-ss69 MPU0 %SYS_UPDATE-RESULT-5:image : Mpu 0 write file to backup file-system
successfully!
Apr 16 2021 03:12:28 BCM_hezi-ss69 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!
```

```
Apr 16 2021 03:12:30 BCM_hezi-ss69 MPU0 %SYS_UPDATE-RESULT-5:Upgrade image to
sp7-g-9.7.1.1(74)(R).pck from ftp: 130.255.168.45 successfully !
```

The above message indicates that the image program 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.

- 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</b> [ <b>device</b> { <i>memberId</i>   <b>all</b> }] <b>mpu</b> [ <b>vrf</b> <i>vrf-name</i> ] <i>dest-ip-address filename</i> [ <b>ftp</b> <i>ftp-username ftp-password</i> ] | Mandatory<br>If the FTP option is not specified, TFTP is used for upgrade by default. |

Upgrade the patch program with the file name sp7-g-9.7.1.1.HP001.pat from the device interface via FTP server 130.255.168.45.

```
Hostname#sysupdate patch mpu 130.255.168.45 sp7-g-9.7.1.1.HP001.pat ftp a a
```

#The device will prompt the following:

```
checking " sp7-g-9.7.1.1.HP001.pat" : ...OK
```

```
downloading "sp7-g-9.7.1.1.HP001.pat" : #OK
```

```
.....(Omitted).....
```

```
%Sysupdate patch finished.
```

```
sysupdate patch result information list:
```

```
-----
Card      result information
-----
```

```
Mpu 0      upgrade successfully!
```

```
sysupdate patch to sp7-g-9.7.1.1.HP001.pat from ftp: 130.255.168.45 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 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 10-5 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><br>[ <b>device</b> { <i>memberId</i>   <b>all</b> } ]<br><b>mpu</b> [ <b>vrf</b> <i>vrf-name</i> ] { <i>dest-ip-address</i> <i>dest-ipv6-address</i> } <i>filename</i> [ <b>ftp</b> <i>ftp-username</i> <i>ftp-password</i> ]<br>[ <b>reload</b> ] | Mandatory<br><br>If the FTP option is not specified, TFTP is used for upgrade by default. |

For example: In standalone mode, upgrade the bootloader program on the MPU via the FTP server 130.255.168.45.

```

Hostname#sysupdate bootloader mpu 130.255.168.45 sz01-bootloader-nl02-9.6.0.3ft15-1.1.18.pck ftp a a
#The device will prompt the following:
checking " sz01-bootloader-nl02-9.6.0.3ft15-1.1.18.pck " : ...OK
downloading " sz01-bootloader-nl02-9.6.0.3ft15-1.1.18.pck " : ####OK
Download " sz01-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! |

#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 10-6 Upgrading the bootloader Program via the Console Port

| Step                      | Command | Description                                                                                                                                                                                                              |
|---------------------------|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Set up the HyperTerminal. | None    | Mandatory<br><br>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<br><br>When the device reboots, press CTRL+C to enter the                                                                                                                                                      |

| Step                                                                                   | Command                       | Description                                                                                                                                                                         |
|----------------------------------------------------------------------------------------|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                        |                               | 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<br>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<br>Enter the mupdate bootloader command in bootloader mode, then select the ymodem protocol in HyperTerminal, 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:
bootloader# mupdate bootloader
Download bootloader start...
run command=loady
## Ready for binary (ymodem) download to 0x20000000 at 115200 bps...
C
Starting ymodem transfer. Press Ctrl+C to cancel.
Transferring sz02sz01-bootloader-nl02-9.6.0.3f15-1.1.18.pck...
 100%  1760 KB    4 KB/sec  00:07:03    0 Errors

## Total Size      = 0x001b83d8 = 1803224 Bytes
Download bootloader OK.
bootloader image check:
..... done
Un-Protected 16 sectors

..... done
Erased 16 sectors
run command=cp.b 200000f0 0x1bc00000 0xc3ea0
Copy to Flash... done
..... done
Protected 16 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.
- 

## 10.2.4 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 10-7 Upgrading Devinfo File via TFTP/FTP

| Step                            | Command | Description |
|---------------------------------|---------|-------------|
| Enter the privileged user mode. | None    | Mandatory   |

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

For example: In standalone mode, upgrade the devinfo file on the MPU via the FTP server 130.255.168.45.

```

Hostname#sysupdate devinfo mpu 130.255.168.45 devInfo_sw_HIT_V2.125 ftp a a
#The device will prompt the following:
checking "devInfo_sw_HIT_V2.125" : ...OK
downloading "devInfo_sw_HIT_V2.125" : #OK
Download "devInfo_sw_HIT_V2.125" (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! |

#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.

---

## 10.2.5 Package file upgrade

The package file contains image, bootloader, and devinfo file, 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 10-8 Upgrading Package File via TFTP/FTP

| Step                            | Command                                                                                                                                                                                                                                                                                      | Description                                                                               |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|
| Enter the privileged user mode. | None                                                                                                                                                                                                                                                                                         | Mandatory                                                                                 |
| Upgrade Package File            | <b>sysupdate package</b> [ <b>device</b><br><i>{ memberId   all }</i> ] [ <b>vrf</b> <i>vrf-name</i> ]<br><i>{ dest-ip-address   dest-ipv6-address }</i><br><i>filename</i> [ <b>ftp</b> <i>ftp-username</i> <i>ftp-</i><br><i>password</i> ] [ <b>no-comparision</b> ]<br>[ <b>reload</b> ] | Mandatory<br><br>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 sp7-g-9.7.1.1(74)(R)-001.pkg FTP a a
```

#The device will prompt the following:

```

Downloading "sp7-g-9.7.1.1(74)(R)-001.pkg" header...OK!
Checking "sp7-g-9.7.1.1(74)(R)-001.pkg" header...OK!

Downloading "sp7-g-9.7.1.1(74)(R)-001.pkg" :
#####OK!
Download "sp7-g-9.7.1.1(74)(R)-001.pkg" (96507023 Bytes) successfully!
Checking package file...OK!
Verify the image...valid
Writing file to
filesystem.....
.....OK!
Start backup ios to raw flash.....
Apr 16 2021 02:46:51 BCM_hezi-ss69 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 02:47:10 BCM_hezi-ss69 MPU0 %SYS_UPDATE-RESULT-5:image : Mpu 0 write file to backup file-system
successfully!
Apr 16 2021 02:47:10 BCM_hezi-ss69 MPU0 %SYS_UPDATE-RESULT-5:image : Mpu 0 upgrade successfully!
%Sysupdate image finished.
Update bootloader start.
.....OK.

%Sysupdate bootloader is in process, please wait...
Apr 16 2021 02:47:15 BCM_hezi-ss69 MPU0 %SYS_UPDATE-RESULT-5:bootloader : Mpu 0 upgrade successfully!
%Sysupdate bootloader finished.
Writing file to filesystem...OK!
.
%Sysupdate devinfo is in process, please wait...
Apr 16 2021 02:47:16 BCM_hezi-ss69 MPU0 %SYS_UPDATE-RESULT-5:devinfo : Mpu 0 upgrade successfully!
%Sysupdate devinfo finished..
%Sysupdate pkgInfo is in process, please wait...
Apr 16 2021 02:47:17 BCM_hezi-ss69 MPU0 %SYS_UPDATE-RESULT-5:pkgInfo : Mpu 0 upgrade successfully!
%Sysupdate pkgInfo finished.

package sysupdate result information list:
-----

sp7-g-9.7.1.1(74)(R).pck sysupdate result information list:
-----

Mpu 0 - upgrade successfully!

sz03-bootloader-cn61-1.0.35.pck sysupdate result information list:
-----

Mpu 0 - 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!
BCM_hezi-ss69#

Apr 16 2021 02:47:19 BCM_hezi-ss69 MPU0 %SYS_UPDATE-RESULT-5:Sysupdate package to sp7-g-9.7.1.1(74)(R)-
001.pkg from ftp: 130.255.168.45 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

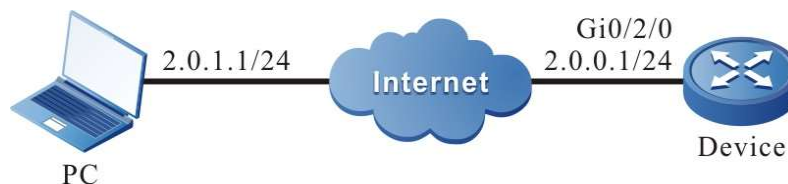


Figure 10-1 Network Topology for Packaged Upgrading of All Supported Software Versions

#### 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 sp28sp28-g-9.66.0.11(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 all upgrade programs included in the packaged upgrade file on the device.

```
%Sysupdate pkgInfo finished.
```

```
package sysupdate result information list:
```

```
-----
```

```
sp7-g-9.7.1.1(74)(R).pck sysupdate result information list:
```

```
-----
```

```
Mpu 0 - upgrade successfully!
```

```
sz03-bootloader-cn61-1.0.35.pck sysupdate result information list:
```

```
-----
```

```
Mpu 0 - 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-comparision" 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 packaged upgrade program via the show package version command.

```
Device#show package version
```

```
package      :sp7-g-9.7.1.1(74)(R)-001.pkg
image        :sp7-g-9.7.1.1(74)(R).pck
bootloader   :sz03-bootloader-cn61-1.0.35.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 command.

```
Device#show system version  brief
```

version information display:

| Module | Online State    | Name   | BootLoader | IOS                      | CMM | PCB | CPLD |
|--------|-----------------|--------|------------|--------------------------|-----|-----|------|
| FPGA   |                 |        |            |                          |     |     |      |
| Mpu 0  | online Start Ok | HIT SW | 1.0.36     | 9.7.1.1(74)(integrity) / | 001 | 105 | /    |

---



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 2.0.0.1 sp7-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-cn61-1.0.35.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 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 mpu 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 the upgrade version is higher than the current running version of the system before upgrade. If the FPGA version is not updated, then the upgrade is not necessary. Please refer to step 10 below to check the current FPGA version of the system.
- 

Step 7: Upgrade CPLD files

#Use sysupdate to upgrade the CPLD program on board.

```
Device#sysupdate cpld mpu 2.0.0.1 pb011_s5830_cpld_clv009.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 8: Upgrade devinfo program

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

```
Device#sysupdate devinfo mpu 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 9: 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 10: 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:  HIT SW
          Status: Start Ok
          Last-Alarm:  Normal
          Card-Port-Num:  54
          Card-SubSlot-Num:  0
          Power-INTF-Status:  Normal
          Power-Card-Status:  On
          Serial No.:  mpu30--;kljhsadi$^#&-['
          Description:
Hardware-Information:
          PCB-Version: 001
          CPLD-Version: 105
Software-Information:
          Bootloader-Version: 1.0.36
          Software-Version: 9.7.1.1(74)(integrity)
Temperature-Information:
          Temperature-State:
                          Switch-Temperature = 63 C
                          Last-Alarm = Normal.
CPU-On-Card-Information:  < 1 CPUs>
          CPU-Idx:  00
          Status:  Normal
          Core-Num:  0002
          Core-State:
          Core-Idx-00
                          Core-Status:  0000
                          Core-Utilization:  18%
          Core-Idx-01
                          Core-Status:  0000
                          Core-Utilization:  0%
          Temperature:
          Temperature-State:
                          Temperature = 48 C
                          Last-Alarm = Normal.
MEM-On-Card-Information:  <1 MEMs>
          MEM-Idx:  00
          MEM-State:
                          BytesFree = 3301539840 bytes
                          BytesAlloc = 859258880 bytes
                          BlocksFree = 5 blocks
                          BlocksAlloc = 364 blocks
                          MaxBlockSizeFree = 58720256 bytes
                          SizeTotal = 4160798720 bytes
DISK-On-Card-Information:  <3 DISKs>
          DISK-Idx:  00
          Type:  Flash
          Status:  Online
          DISK-State:
```



```

SizeTotal = 3964465152 bytes
SizeFree = 3333177344 bytes
CPLD-On-Card-Information: <2 CPLDs>
CPLD-Idx: 00
Info-Struct:
    version = 105
CPLD-Idx: 01
Info-Struct:
    version = 105
-----
STATISTICS:      1 IN, 0 OUT, 0 IERR, 0 OERR

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

```

---



Note:

- 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

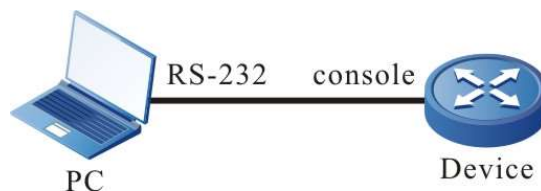


Figure 10-3 Using the Console Port to Upgrade the bootloader Program

## 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#srate 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.

```
download bootloader via y modem protocol.....CCCCC
```

```
Starting ymodem transfer. Press Ctrl+C to cancel.
```

```
Transferring sz03-bootloader-cn61-1.0.34.pck...
```

```
100% 1760 KB 4 KB/sec 00:07:03 1 Errors
```

```
## Total Size = 0x001b83d8 = 1803224 Bytes
```

```
success!
```

```
Update bootloader start...
```

```
Erase Master Flash OK ...
```

```
\Flash Program OK ...
```

```
Verifying flash data...
```

```
Verify OK ...
```

```
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 1.0.34 (Build time: Apr 02 2021 - 08:38:15)

Warm boot from slave sector

Press ctrl+c to enter bootloader mode: 0

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. |
| 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<br><br>After the device is powered on, press and 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<br><br>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><br><i>filename local-ip-addr</i><br><i>host-ip-addr [gatewayip]</i><br><i>[ netmask]</i><br><br><b>change</b> <i>index[0~3]</i> <b>flash0</b><br><i>filename</i> | Mandatory<br><br>The first line of the command is the network startup configuration parameters, if you upgrade across network segments, you need to add the gateway and mask.<br><br>The second line of the command is the startup configuration parameters for flash storage device. |



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 Upgrade bootloader Program

| Step                                    | Command                                                                                        | Description                                                                                                                                                           |
|-----------------------------------------|------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Enter the bootloader configuration mode | None                                                                                           | Mandatory<br>After the device is powered on, press and hold "ctrl+c" to enter the bootloader configuration mode; after entering, the prompt message is: "bootloader#" |
| Start tftp server on the PC.            |                                                                                                | Mandatory<br>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<br>Upgrade the PCK file of bootloader via tftp server                                                                                                       |
| 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</b> <i>index[0~4]</i> | Display startup parameters information specified by index.                                               |
| <b>boot</b> <i>index[0~4]</i>  | Load the startup parameters information specified by index.                                              |
| <b>clear</b> <i>index[0~3]</i> | Clear the startup parameters information specified by index.                                             |
| <b>grate</b>                   | Obtain data on the speed rate of the current serial port.                                                |
| <b>Srate</b> <i>ratenum</i>    | 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 sp7-g-9.7.1.1(70)(T)(v3.9.0.255)-dbg.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.

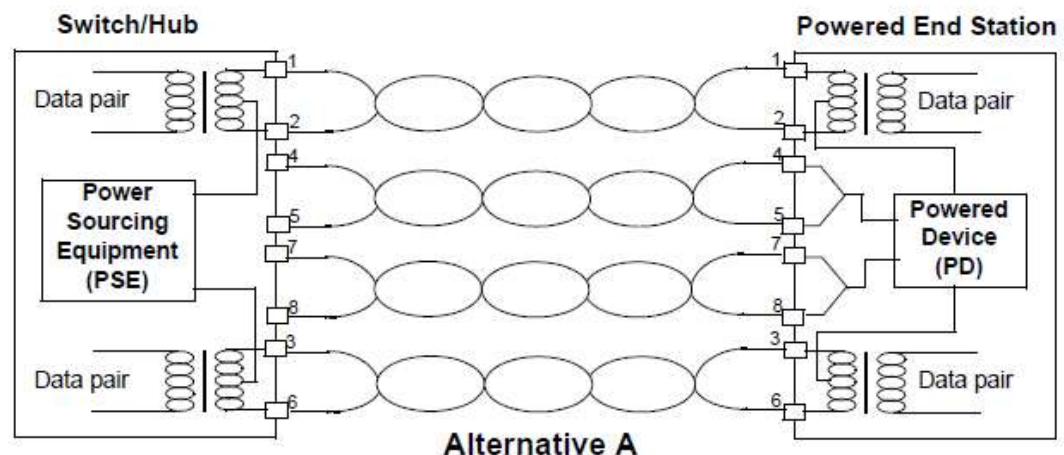


Figure 12-1 Alternative A Power Supply Mode with 10BASE-T and 100BASE-TX

## 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.

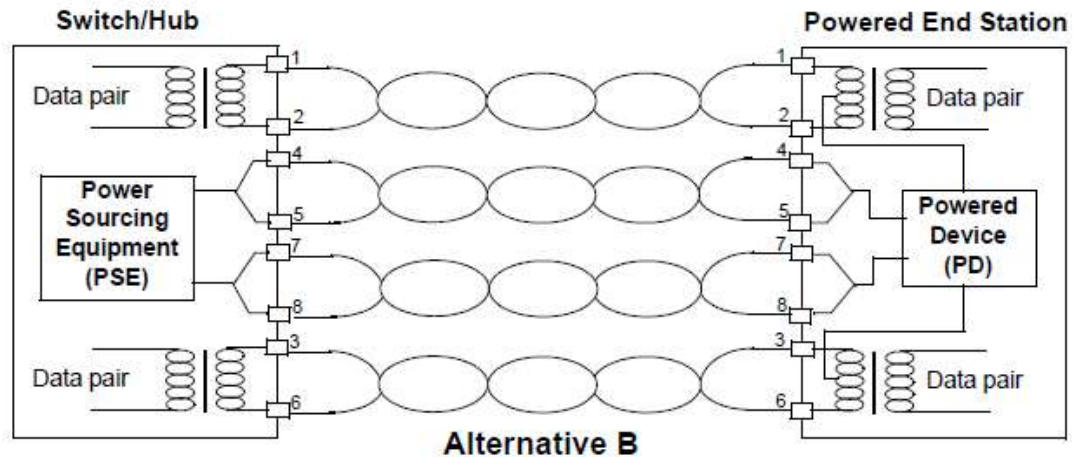


Figure 12-2 Alternative B Power Supply Mode with 10BASE-T and 100BASE-TX

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:

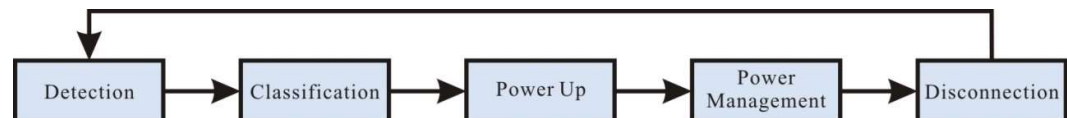


Figure 12-3 PSE Power Supply Process

- **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
	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

Configuration Task	
	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
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>	-
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</b> { <b>all</b>   <i>system-id</i> { <b>all</b>   <i>subsystem-id</i> } } <i>power-value</i>	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 12-7 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</b> { <b>all</b>   <i>system-id</i> { <b>all</b>   <i>subsystem-id</i> } } <i>guard-band-value</i>	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 12-8 Configuring the Maximum Output Power Limit Mode of an Interface

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 the Maximum Output Power Limit Mode of an Interface	<b>power threshold-mode</b> { <b>classification</b>   <b>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 12-9 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 12-10 Configuring a PoE Power Management Mode

Step	Command	Description
Enter the global configuration mode.	<b>configure terminal</b>	-
Configure a PoE Power Management Mode	<b>power manage { all   system-id { all   subsystem-id } } { dynamic-fifs   dynamic-priority   static-fifs   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 { all   system-id { all   subsystem-id } } 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 interface-name</b>	-
Configure the Power Supply Priority of an Interface	<b>power priority { critical   high   medium   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>	-
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</b> { <b>ac</b>   <b>dc</b> }	Optional By default, the power failure detection mode is AC.



#### 说明:

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 12-17 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 12-18 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 12-19 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 12-20 PoE Monitoring and Maintaining

Command	Description
<b>show power { manage   summary   configure interface <i>interface-name</i>   detect interface <i>interface-name</i>   pd-status interface <i>interface-name</i>   system-to-port [ <i>system-id</i> ]   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 <i>interface-name</i></b>	-
Enable interface PDI function.	<b>pdi enable</b>	Mandatory By default, the interface PDI function is not enabled.

## 13.3 Configure the ARP message delivery interval.

Table 13-2 Configuring the Interface ARP Message Delivery Interval



Step	Command	Description
Enter the L2/L3 Ethernet interface configuration mode.	<b>interface</b> <i>interface-name</i>	-
Configure the interface ARP message delivery interval.	<b>pdi inspection-interval</b>	Optional By default, the interface arp message delivery interval is 3s.

## 13.4 Configure the number of retries for ARP message delivery.

Table 13-3 Configuring the Number of Retries for ARP Message 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 message delivery of an interface.	<b>pdi inspection-retry</b>	Optional By default, the number of retries for ARP message 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</b> <i>ip-entry</i> <b>interface</b> <i>interface-name</i>	Display PDI global structure, port summary information and detailed information, etc.

Command	Description
<b>statistic statistic interface</b> <i>interface-name</i> }	

# 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
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 Corresponding to User Roles

	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	All commands other than	Histroy	NO	OK

administrator	operation log and data log	configuration and operation		
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</b> <i>role-name</i>	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.
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

Step	Command	Description
		<p>user role does not have any privileges.</p> <p>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.</p> <p>Rules with smaller rule IDs have higher priority.</p>

## 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> <b>class</b> <b>manager</b>	<p>Mandatory.</p> <p>By default, no administrator user is configured.</p>

### 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</b> 0 <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</b> { <i>ssh</i>   <i>telnet</i>   <b>console</b>   <b>ftp</b>   <b>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.
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</b>

Step	Command	Description
		<b>automatically.</b>
Configure options for users to automatically execute commands.	<b>autocommand-option { nohangup [ delay <i>delay-time-number</i> ] [delay <i>delay-time-number</i> [ 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 <i>user-live-time</i></b>	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 <i>max-try-time-number</i></b>	Optional. By default, user management does not set limits on the maximum number of attempts.
Configure the maximum number of online sessions for the same user.	<b>max-online-num <i>user-number</i></b>	Optional. 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>filesystem-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 <i>directory</i></b>	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 len  with user-name-check   composition type-number type-number }</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 lifetime	<b>password-control lifetime</b> <i>user-live-time</i>	Optional.  By default, no limit is set on user lifetime.
Configure the maximum number of consecutive login authentication failures for administrator users	<b>password-control max-try-time</b> <b>max-try-time-number</b>	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

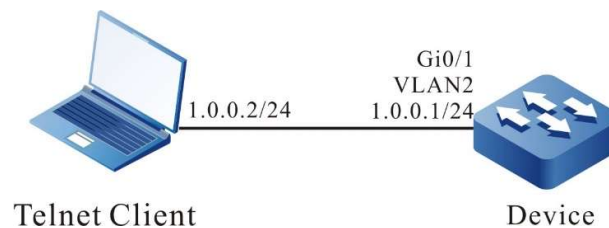


Figure 14-1 Network Topology for Configuring the Network Administrator User Group

#### 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 messages 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 messages across the network segments. When the DHCP server receives the DHCP discovery messages, 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 message 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.

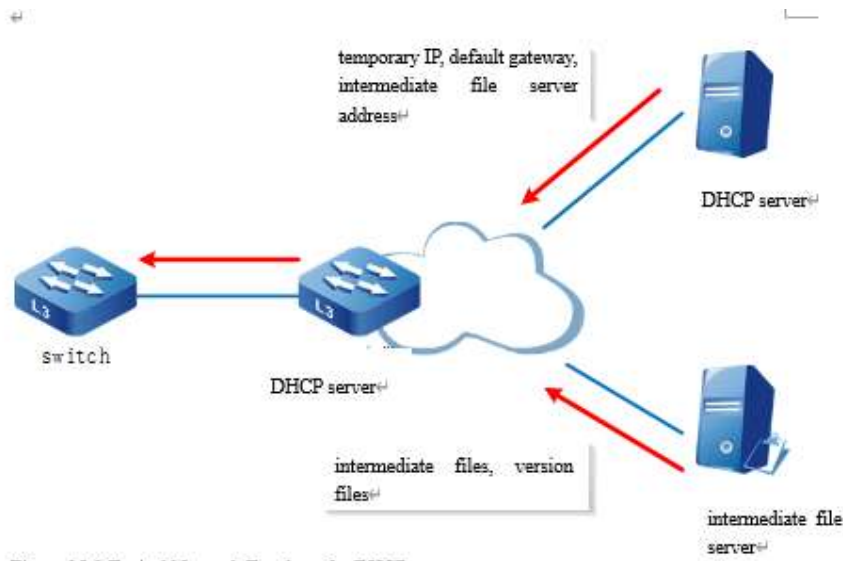
Figure 15-1 Typical Network Topology for DHCP

**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 segments, it needs to forward the DHCP interaction messages through the DHCP relay to the DHCP server.

**Intermediate file server:** Used to store intermediate files (intermediate file type in binary 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 15-2ZTP 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 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

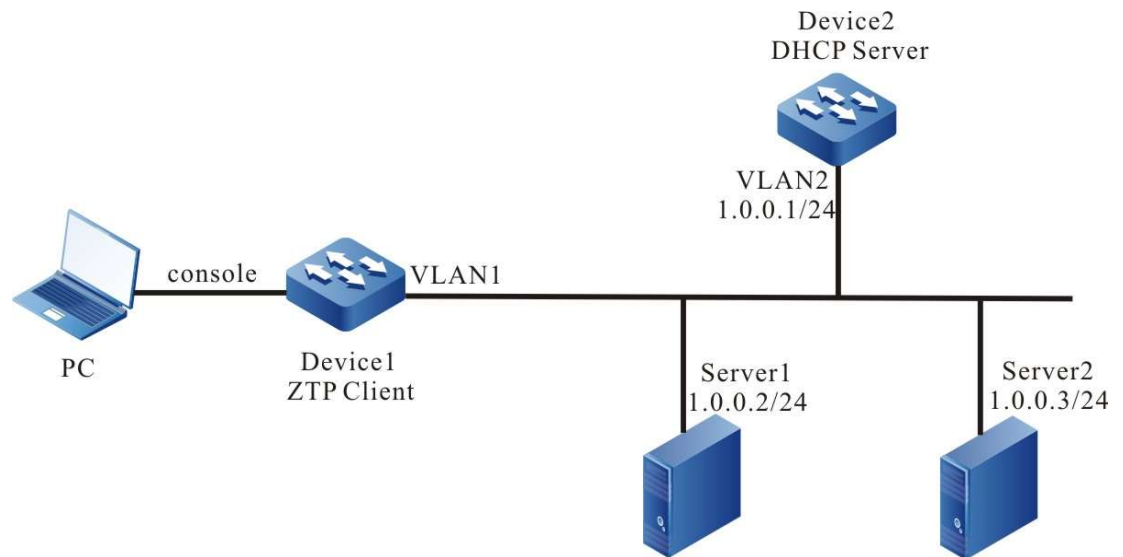


Figure 15-2 Network Topology of Device Using Common Intermediate Files for Zero-configuration Deployment via DHCP

### 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.

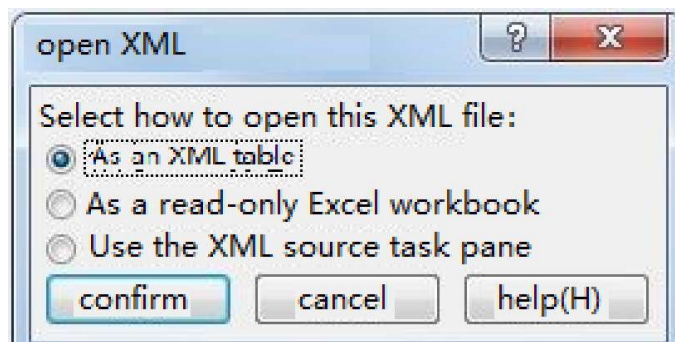


Figure 15-3 Determined as XML Table

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	E	F
1	Serial-Number	Image-File	Image-File-MD5	Config-File	Config-File-MD5	Description
2	example 1:123456789	xxx.pck	xxx	startup	xxx	
3	example 1:123456789			startup		

Figure 15-4Editing 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

May  6 2020 15:04:19 Device1 MPU0 %ZTP-5:Now starting DHCP upgrade...
May  6 2020 15:04:19 Device1 MPU0 %ZTP-5: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.

May  6 2020 15:04:23 Device1 MPU0 %ZTP-5:Press (ctrl + c) to abort Dhcp Upgrade

#Get the address successfully, download the common intermediate files

May  6 2020 15:06:29 Device1 MPU0 %DHCP-ASSIGNED_EXT-5:Interface vlan1 assigned DHCP address 1.0.0.4, mask
255.255.255.0.
May  6 2020 15:06:31 Device1 MPU0 %ZTP-5:Dhcp Upgrade DHCP discovery phase success
May  6 2020 15:06:31 Device1 MPU0 %ZTP-5:Start to download temp file ztp.xml

#Parse intermediate files and download version information

May  6 2020 15:06:56 Device1 MPU0 %ZTP-5:Download temp file ztp.xml is success
May  6 2020 15:06:56 Device1 MPU0 %ZTP-5:Start to parse temp file...
May  6 2020 15:06:56 Device1 MPU0 %ZTP-5:parse temp file is success
May  6 2020 15:06:56 Device1 MPU0 %ZTP-5:Start to download the Image file ztp.pck
```

#Download version and configuration file successfully, reboot the device automatically via ZTP

```
May 6 2020 15:14:09 Device1 MPU0 %SYS_UPDATE-RESULT-5:image : Mpu 0 upgrade successfully!
May 6 2020 15:14:11 Device1 MPU0 %ZTP-5:Download the Image file is success
May 6 2020 15:14:11 Device1 MPU0 %ZTP-5:Start to download the config file startup_ztp...
May 6 2020 15:14:12 Device1 MPU0 %ZTP-5:Download the config file is success
May 6 2020 15:14:12 Device1 MPU0 %ZTP-5:DHCP upgrade is success
May 6 2020 15:14:12 Device1 MPU0 %ZTP-5: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 and TFTP, 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 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

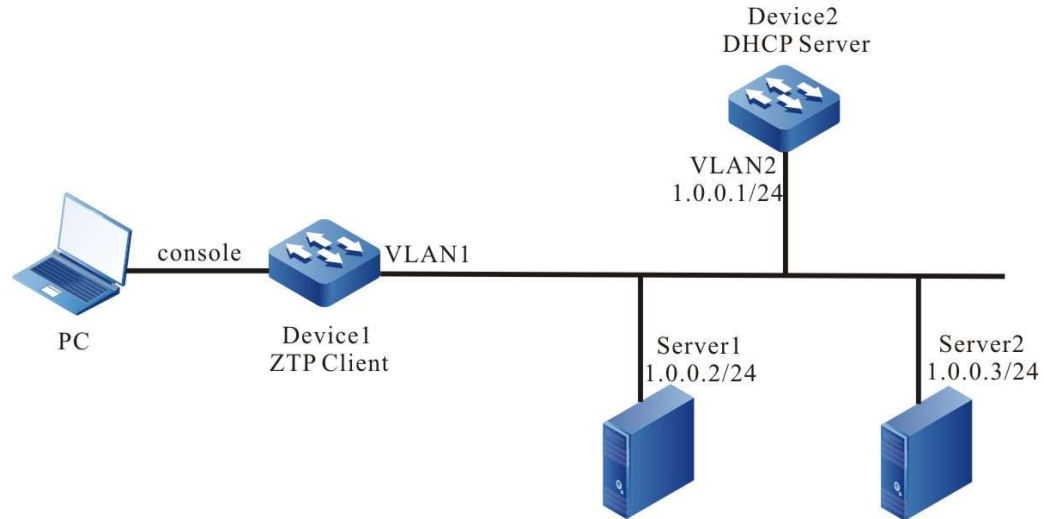


Figure 15- 5 Network Topology of Device Using Python Intermediate Files for Zero-configuration Deployment via DHCP

### Configuration Steps

- Step 1: Configure the FTP server and place the intermediate files (e.g. ztp.py), version files and device configuration files 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 = {
    'NSS8900' : '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

May  6 2020 15:04:19 Device1MPU0 %ZTP-5:Now starting DHCP upgrade...
May  6 2020 15:04:19 Device1MPU0 %ZTP-5: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.

May  6 2020 15:04:23 Device1MPU0 %ZTP-5:Press (ctrl + c) to abort Dhcp Upgrade

#Get the address successfully, download the common intermediate files

May  6 2020 16:09:42 Device1 MPU0 %DHCP-ASSIGNED_EXT-5:Interface vlan1 assigned DHCP address 1.0.0.4, mask
255.255.255.0.
May  6 2020 16:09:56 Device1 MPU0 %ZTP-5:Dhcp Upgrade DHCP discovery phase success
May  6 2020 16:09:56 Device1 MPU0 %ZTP-5:Start to download temp file ztp.py...

```

May 6 2020 16:09:56 Device1 MPU0 %ZTP-5:Download temp file ztp.py is success

#### #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/12345.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

May 6 2020 16:16:15 MPU0 %SYS\_UPDATE-RESULT-5:image : Mpu 0 upgrade successfully!  
Set boot image 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.

May 6 2020 16:16:18 Device1 MPU0 %ZTP-5:script execute success

May 6 2020 16:16:18 Device1 MPU0 %ZTP-5: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:  
TFTP server IP: 1.0.0.2  
Temporary file name: ztp.py

Current ztp method: None upgrade method

Next ztp state: disable



#### Note:

- The device obtains the file download mode through option66 of DHCP protocol. It supports FTP and TFTP, 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

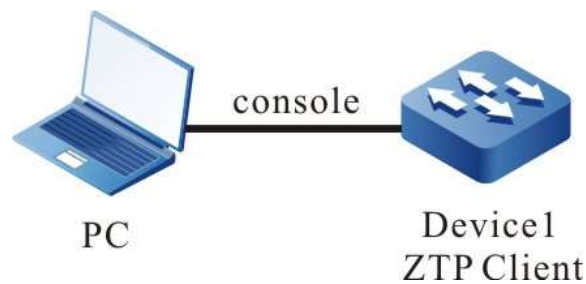


Figure 15-6 Network Topology of Device Using Common Intermediate Files for Zero-configuration Deployment via USB

#### 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.

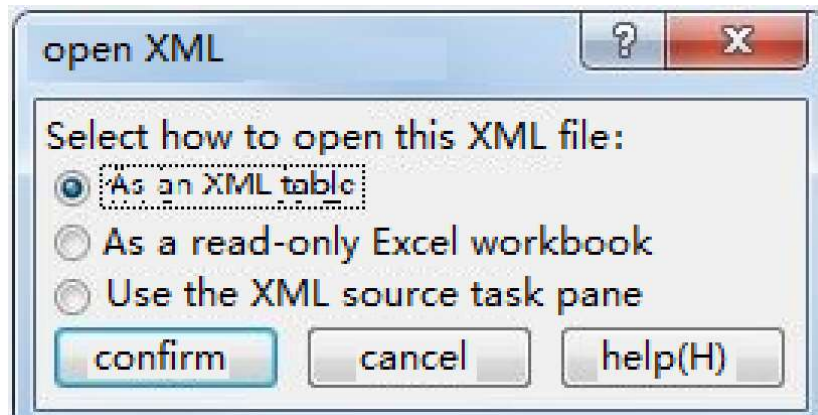


Figure 15-9 Determined as XML Table

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	
1	Serial-Number	Image-File	Image-File-MD5	Config
2	example_1:123456789	xxx.pck	xxx	startup
3	example_1:123456789			startup

Figure 15-7 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 Device1MPU0 %ZTP-USB\_UPGRADE-5:Now starting USB upgrade...

#Find and parse intermediate files

May 6 2020 15:16:15 Device1MPU0 %ZTP-USB\_UPGRADE-5:Start to copy the temporary file /usb/ztp\_config.xml...  
May 6 2020 15:16:15 Device1MPU0 %ZTP-USB\_UPGRADE-5:Copy the temporary file is success.  
May 6 2020 15:16:15 Device1MPU0 %ZTP-USB\_UPGRADE-5:Start to parse the temporary file /flash/ztp\_config.xml

#Upgraded versions and configurations

May 6 2020 15:16:15 Device1MPU0 %ZTP-USB\_UPGRADE-5:Parse temporary file is success  
May 6 2020 15:19:53 Device1MPU0 %ZTP-USB\_UPGRADE-5:Sysupdate image is success  
May 6 2020 15:19:53 Device1 MPU0 %ZTP-USB\_UPGRADE-5:Start to copy config...  
May 6 2020 15:19:54 Device1 MPU0 %ZTP-USB\_UPGRADE-5:Copy config is success

#Reboot after upgrade

May 6 2020 15:19:54 Device1 MPU0 %ZTP-USB\_UPGRADE-4: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

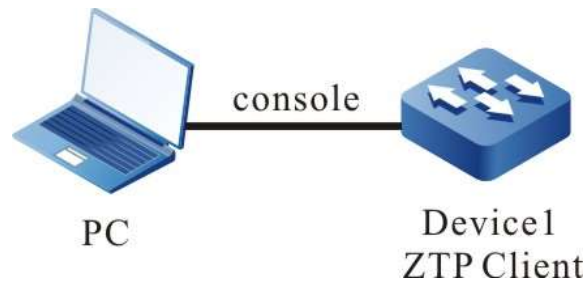


Figure 15-8 Network Topology of Device Using Python Intermediate Files for Zero-configuration Deployment via USB

#### 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 = {
    'NSS8900' : '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 %ZTP-5:Now starting USB upgrade...

#Find and parse intermediate files

Apr 30 2020 11:10:12 Device1 MPU0 %ZTP-5:Start to copy the temporary file /usb/ztp\_script.py...  
Apr 30 2020 11:10:12 Device1 MPU0 %ZTP-5:Copy the temporary file is success.  
Apr 30 2020 11:10:12 Device1 MPU0 %ZTP-5: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: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 %ZTP-5:script execute success  
Apr 30 2020 11:13:54 Device1 MPU0 %ZTP-4: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 and TFTP, 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 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

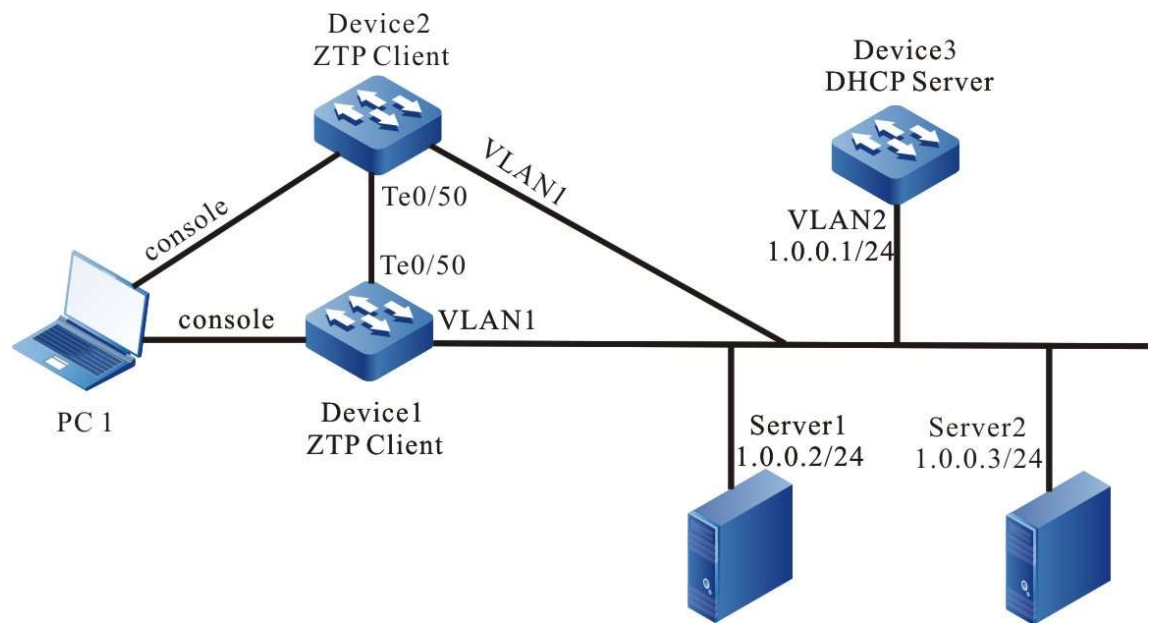


Figure 15-9 Network Topology of ZTP using python intermediate files to automatically complete stacking via DHCP

### 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 = {

'NSS8900' : '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.cfg.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. cfg.md5.

The stacking section of the configuration file must be included with !VST\_CONFIG\_BEGIN and !VST\_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
```

```
!slot_0_NSS8900-08(V1)
```

```
!vsl mode
```

```
!slot 0/0
```

```
interface tengigabitethernet1/0/50
```

```
vsl-channel 1/1 mode on
```

```
exit
```

```
!end
```

```
!VST_CONFIG_END
```

The configuration file of Device2 contains

```
!VST_CONFIG_BEGIN
```

```
!mode vsl information
```

```
vsl-channel 0/1
```

```
exit
```

```
!mode vsl end
```

```
!slot_0_NSS8900-08(V1)
```

```
!vsl mode
```

```
!slot 0/0
```

```
interface tengigabitethernet0/0/50
```

```
vsl-channel 0/1 mode on
```

```
exit
```

```
!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

```
May 6 2020 15:04:19 Device1 MPU0 %ZTP-5:Now starting DHCP upgrade...
May 6 2020 15:04:19 Device1 MPU0 %ZTP-5: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.

```
May 6 2020 15:04:23 Device1 MPU0 %ZTP-5:Press (ctrl + c) to abort Dhcp Upgrade
```

#### #Get the address successfully, download the common intermediate files

```
May 6 2020 16:09:42 Device1 MPU0 %DHCP-ASSIGNED_EXT-5:Interface vlan1 assigned DHCP address 1.0.0.4, mask 255.255.255.0.
May 6 2020 16:09:56 Device1 MPU0 %ZTP-5:Dhcp Upgrade DHCP discovery phase success
May 6 2020 16:09:56 Device1 MPU0 %ZTP-5:Start to download temp file ztp.py...
May 6 2020 16:09:56 Device1 MPU0 %ZTP-5:Download temp file ztp.py is success
```

#### #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 30 2020 09:45:32 Device1 MPU0 %ZTP-5:script execute success
Apr 30 2020 09:45:32 Device1 MPU0 %ZTP-5:System will rebooted by DHCP upgrade
```

The device Device2:

#See that the device enters the ZTP process through logs and sends DHCP requests

```
May 6 2020 15:04:19 Device2 MPU0 %ZTP-5:Now starting DHCP upgrade...
May 6 2020 15:04:19 Device2 MPU0 %ZTP-5: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.

```
May 6 2020 15:04:23 Device2 MPU0 %ZTP-5:Press (ctrl + c) to abort Dhcp Upgrade
```

#Get the address successfully, download the common intermediate files

```
May 6 2020 16:09:42 Device2 MPU0 %DHCP-ASSIGNED_EXT-5:Interface vlan1 assigned DHCP address 1.0.0.5, mask 255.255.255.0.
May 6 2020 16:09:56 Device2 MPU0 %ZTP-5:Dhcp Upgrade DHCP discovery phase success
May 6 2020 16:09:56 Device2 MPU0 %ZTP-5:Start to download temp file ztp.py...
May 6 2020 16:09:56 Device2 MPU0 %ZTP-5:Download temp file ztp.py is success
```

#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 30 2020 09:45:32 Device2 MPU0 %ZTP-5:script execute success
Apr 30 2020 09:45:32 Device2 MPU0 %ZTP-5: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 information:  
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 7
domain 101
exit
!mode member end
```

```
!mode vsl information
vsl-channel 0/1
exit
vsl-channel 1/1
exit
!mode vsl end
```

```
!slot_0_NSS8900-08(V1)
!vsl mode
!slot 0/0
interface tengigabitethernet0/0/50
vsl-channel 0/1 mode on
exit
!end
```

```
!slot_14_NSS8900-08(V1)
!vsl mode
!slot 7/0
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 and TFTP, 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 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.
-