Reference Manual

Command Line Interface
Industrial ETHERNET Switch
RSB20, OCTOPUS OS20/OS24 Managed
The naming of copyrighted trademarks in this manual, even when not specially indicated, should not be taken to mean that these names may be considered as free in the sense of the trademark and tradename protection law and hence that they may be freely used by anyone.

© 2012 Hirschmann Automation and Control GmbH

Manuals and software are protected by copyright. All rights reserved. The copying, reproduction, translation, conversion into any electronic medium or machine scannable form is not permitted, either in whole or in part. An exception is the preparation of a backup copy of the software for your own use. For devices with embedded software, the end-user license agreement on the enclosed CD applies.

The performance features described here are binding only if they have been expressly guaranteed in the contract. This publication has been created by Hirschmann Automation and Control GmbH according to the best of our knowledge. Hirschmann reserves the right to change the contents of this manual without prior notice. Hirschmann can give no guarantee in respect of the correctness or accuracy of the details in this publication.

Hirschmann can accept no responsibility for damages, resulting from the use of the network components or the associated operating software. In addition, we refer to the conditions of use specified in the license contract.

Printed in Germany 6/11/12

Hirschmann Automation and Control GmbH
Stuttgarter Str. 45-51
72654 Neckartenzlingen
Germany
Tel.: +49 1805 141538
Content

Quick Start up
Quick Starting the Switch 12
System Info and System Setup 13

1 Command Structure 19
1.1 Format 20
  1.1.1 Command 20
  1.1.2 Parameters 21
  1.1.3 Values 21
  1.1.4 Conventions 23
  1.1.5 Annotations 24
  1.1.6 Special keys 25

2 Mode-based CLI 27
2.1 Mode-based Topology 28
2.2 Mode-based Command Hierarchy 29
2.3 Flow of Operation 31
2.4 “No” Form of a Command 33
  2.4.1 Support for “No” Form 33
  2.4.2 Behavior of Command Help (“?”) 33

3 CLI Commands: Base 35
3.1 System Information and Statistics Commands 36
  3.1.1 show arp switch 36
  3.1.2 show bridge aging-time 36
  3.1.3 show bridge fast-link-detection 37
  3.1.4 show config-watchdog 37
  3.1.5 show device-status 38
  3.1.6 show eventlog 39
  3.1.7 show interface 40
  3.1.8 show interface ethernet 42
  3.1.9 show interface switchport 49
  3.1.10 show logging 49
3.1.1 show mac-addr-table 50
3.1.12 show signal-contact 51
3.1.13 show slot 52
3.1.14 show running-config 53
3.1.15 show sysinfo 53

3.2 Class of Service (CoS) Commands 56
3.2.1 classofservice dot1p-mapping 57
3.2.2 classofservice ip-dscp-mapping 58
3.2.3 classofservice trust 59
3.2.4 show classofservice dot1p-mapping 60
3.2.5 show classofservice ip-dscp-mapping 61
3.2.6 show classofservice trust 62

3.3 Management Commands 63
3.3.1 bridge aging-time 63
3.3.2 bridge fast-link-detection 64
3.3.3 network javascriptmode 64
3.3.4 network parms 65
3.3.5 network protocol 65
3.3.6 network priority 66
3.3.7 serial timeout 67
3.3.8 set prompt 68
3.3.9 show network 68
3.3.10 show serial 70
3.3.11 show snmp-access 70
3.3.12 show snmpcommunity 71
3.3.13 show snmptrap 72
3.3.14 show trapflags 73
3.3.15 snmp-access global 74
3.3.16 snmp-access version 75
3.3.17 snmp-server 76
3.3.18 snmp-server community 77
3.3.19 snmp-server community ipaddr 78
3.3.20 snmp-server community ipmask 79
3.3.21 snmp-server community mode 80
3.3.22 snmp-server community ro 81
3.3.23 snmp-server community rw 81
3.3.24 snmp-server location 81
3.3.25 snmp-server sysname 82
3.3.26 snmp-server enable traps 82
3.3.27 snmp-server enable traps chassis 83
### 3.3.28 snmp-server enable traps l2redundancy

3.3.29 snmp-server enable traps linkmode

3.3.30 snmp-server enable traps stpmode

3.3.31 snmptrap

3.3.32 snmptrap ipaddr

3.3.33 snmptrap mode

3.3.34 snmptrap snmpversion

### 3.4 Syslog Commands

3.4.1 logging buffered

3.4.2 logging buffered wrap

3.4.3 logging cli-command

3.4.4 logging console

### 3.5 Device Configuration Commands

3.5.1 auto-negotiate

3.5.2 cable-crossing

3.5.3 auto-negotiate all

3.5.4 macfilter

3.5.5 macfilter adddest

3.5.6 macfilter adddest all

3.5.7 monitor session <session-id>

3.5.8 monitor session <session-id> mode

3.5.9 monitor session <session-id> source/destination

3.5.10 set igmp (Global Config Mode)

3.5.11 set igmp (Interface Config Mode)

3.5.12 set igmp aging-time-unknown

3.5.13 set igmp automatic-mode

3.5.14 set igmp forward-all

3.5.15 set igmp forward-unknown

3.5.16 set igmp static-query-port

3.5.17 set igmp groupmembershipinterval

3.5.18 set igmp interfacemode

3.5.19 set igmp lookup-interval-unknown

3.5.20 set igmp lookup-resp-time-unknown

3.5.21 set igmp maxresponse

3.5.22 set igmp querier max-response-time

3.5.23 set igmp querier protocol-version

3.5.24 set igmp querier status

3.5.25 set igmp querier tx-interval

3.5.26 set igmp query-ports-to-filter

3.5.27 selftest ramtest
3.5.28 selftest reboot-on-error 117
3.5.29 show igmp-snooping 118
3.5.30 show mac-filter-table igmp-snooping 120
3.5.31 show mac-filter-table multicast 121
3.5.32 show mac-filter-table static 122
3.5.33 show mac-filter-table staticfiltering 123
3.5.34 show mac-filter-table stats 124
3.5.35 show monitor session 125
3.5.36 show port 126
3.5.37 show selftest 127
3.5.38 shutdown 128
3.5.39 shutdown all 129
3.5.40 snmp trap link-status 130
3.5.41 snmp trap link-status all 131
3.5.42 spanning-tree bpdumigrationcheck 132
3.5.43 speed 133

3.6 User Account Management Commands 135
3.6.1 show login session 135
3.6.2 show users 136
3.6.3 users defaultlogin 137
3.6.4 users login <user> 138
3.6.5 users access 139
3.6.6 users name 140
3.6.7 users passwd 141
3.6.8 users snmpv3 accessmode 142
3.6.9 users snmpv3 authentication 143

3.7 System Utilities 145
3.7.1 clear eventlog 145
3.7.2 traceroute 146
3.7.3 clear arp-table-switch 146
3.7.4 clear config 147
3.7.5 clear config factory 147
3.7.6 clear counters 147
3.7.7 clear hiper-ring 148
3.7.8 clear igmp-snooping 148
3.7.9 clear mac-addr-table 149
3.7.10 clear pass 149
3.7.11 clear signal-contact 150
3.7.12 clear traplog 151
Content

3.7.13 config-watchdog
3.7.14 copy
3.7.15 device-status connection-error
3.7.16 device-status monitor
3.7.17 logout
3.7.18 ping
3.7.19 signal-contact connection-error
3.7.20 signal-contact
3.7.21 reboot
3.7.22 reload

3.8 LLDP - Link Layer Discovery Protocol
3.8.1 show lldp
3.8.2 show lldp config
3.8.3 show lldp config chassis
3.8.4 show lldp config chassis admin-state
3.8.5 show lldp config chassis notification-interval
3.8.6 show lldp config chassis re-init-delay
3.8.7 show lldp config chassis tx-delay
3.8.8 show lldp config chassis tx-hold-mult
3.8.9 show lldp config chassis tx-interval
3.8.10 show lldp config port
3.8.11 show lldp config port tlv
3.8.12 show lldp remote-data
3.8.13 lldp
3.8.14 lldp config chassis admin-state
3.8.15 lldp config chassis notification-interval
3.8.16 lldp config chassis re-init-delay
3.8.17 lldp config chassis tx-delay
3.8.18 lldp config chassis tx-hold-mult
3.8.19 lldp config chassis tx-interval
3.8.20 clear lldp config all
3.8.21 lldp admin-state
3.8.22 lldp fdb-mode
3.8.23 lldp hm-mode
3.8.24 lldp max-neighbors
3.8.25 lldp notification
3.8.26 lldp tlv link-aggregation
3.8.27 lldp tlv mac-phy-config-state
3.8.28 lldp tlv max-frame-size
3.8.29 lldp tlv mgmt-addr
3.8.30 lldp tlv port-desc 176
3.8.31 lldp tlv gmrp 177
3.8.32 lldp tlv igmp 177
3.8.33 lldp tlv portsec 177
3.8.34 lldp tlv ptp 178
3.8.35 lldp tlv protocol 178
3.8.36 lldp tlv sys-cap 178
3.8.37 lldp tlv sys-desc 179
3.8.38 lldp tlv sys-name 179
3.8.39 name 179

3.9 SNTP - Simple Network Time Protocol 181
3.9.1 show sntp 181
3.9.2 show sntp anycast 182
3.9.3 show sntp client 183
3.9.4 show sntp operation 184
3.9.5 show sntp server 184
3.9.6 show sntp status 185
3.9.7 show sntp time 185
3.9.8 no sntp 186
3.9.9 sntp anycast address 186
3.9.10 sntp anycast transmit-interval 187
3.9.11 sntp client accept-broadcast 187
3.9.12 sntp client disable-after-sync 188
3.9.13 sntp client offset 188
3.9.14 sntp client request-interval 189
3.9.15 no sntp client server 189
3.9.16 sntp client server primary 189
3.9.17 sntp client server secondary 190
3.9.18 sntp client threshold 191
3.9.19 sntp operation 192
3.9.20 sntp server disable-if-local 193
3.9.21 sntp time system 193

3.10 PTP - Precision Time Protocol 195
3.10.1 show ptp 195
3.10.2 ptp clock-mode 195
3.10.3 ptp operation 196

3.11 PoE - Power over Ethernet 197
3.11.1 show inlinepower 197
3.11.2 inlinepower (Global Config Mode) 197
3.11.3 inlinepower (Interface Config Mode) 198

4 CLI Commands: Switching 199

4.1 Spanning Tree Commands 201
  4.1.1 show spanning-tree 201
  4.1.2 show spanning-tree interface 203
  4.1.3 show spanning-tree mst detailed 204
  4.1.4 show spanning-tree mst port detailed 206
  4.1.5 show spanning-tree mst port summary 209
  4.1.6 show spanning-tree summary 210
  4.1.7 show spanning-tree vlan 211
  4.1.8 spanning-tree 212
  4.1.9 spanning-tree auto-edgeport 213
  4.1.10 spanning-tree configuration name 214
  4.1.11 spanning-tree configuration revision 215
  4.1.12 spanning-tree edgeport 216
  4.1.13 spanning-tree forceversion 217
  4.1.14 spanning-tree forward-time 218
  4.1.15 spanning-tree hello-time 219
  4.1.16 spanning-tree max-age 220
  4.1.17 spanning-tree max-hops 221
  4.1.18 spanning-tree mst 222
  4.1.19 spanning-tree mst priority 224
  4.1.20 spanning-tree mst vlan 225
  4.1.21 spanning-tree port mode 226
  4.1.22 spanning-tree port mode all 227
  4.1.23 spanning-tree stp-mrp-mode 228

4.2 MRP 229
  4.2.1 show mrp 229
  4.2.2 show mrp current-domain 230
  4.2.3 mrp current-domain 231
  4.2.4 mrp delete-domain 232
  4.2.5 mrp new-domain 233

4.3 HIPER-Ring 235
  4.3.1 show hiper-ring 236
  4.3.2 hiper-ring 237
  4.3.3 hiper-ring mode 238
  4.3.4 hiper-ring port primary 238
  4.3.5 hiper-ring port secondary 239
4.3.6 hiper-ring recovery-delay 239

4.4 DHCP Relay Commands 241
4.4.1 show dhcp-relay 241
4.4.2 dhcp-relay (Global Config Mode) 242
4.4.3 dhcp-relay (Interface Config Mode) 243

5 CLI Commands: Security 245

5.1 Security Commands 247
5.1.1 authentication login 247
5.1.2 show authentication 249
5.1.3 show authentication users 250
5.1.4 show users authentication 251
5.1.5 users login 252

5.2 HTTP Commands 253
5.2.1 ip http server 253

6 Glossary 255

7 Index 269

8 Further support 273
Quick Start up

The CLI Quick Start up details procedures to quickly become acquainted with the software.
Quick Starting the Switch

- Read the device Installation Guide for the connectivity procedure. In-band connectivity allows access to the software locally or from a remote workstation. The device must be configured with IP information (IP address, subnet mask, and default gateway).

- Turn the Power on.

- Allow the device to load the software until the login prompt appears. The device’s initial state is called the default mode.

- When the prompt asks for operator login, execute the following steps:
  - Type the word `admin` in the login area. Since a number of the Quick Setup commands require administrator account rights, we recommend logging into an administrator account. Press the enter key.
  - Enter the state on delivery password `private`.
  - Press the enter key
  - The CLI User EXEC prompt will be displayed.
    User EXEC prompt:
    (Hirschmann Product) >
  - Use “enable” to switch to the Privileged EXEC mode from User EXEC.
    Privileged EXEC prompt:
    (Hirschmann Product) #
  - Use “configure” to switch to the Global Config mode from Privileged EXEC.
    Global Config prompt:
    (Hirschmann Product) (Config)#
  - Use “exit” to return to the previous mode.
System Info and System Setup

This chapter informs you about:

- Quick Start up Software Version Information
- Quick Start up Physical Port Data
- Quick Start up User Account Management
- Quick Start up IP Address
- Quick Start up Uploading from Switch to Out-of-Band PC (Only XMODEM)
- Quick Start up Downloading from Out-of-Band PC to Switch (Only XMODEM)
- Quick Start up Downloading from TFTP Server
- Quick Start up Factory Defaults
■ Quick Start up Physical Port Data

<table>
<thead>
<tr>
<th>Command</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>show port all (in Privileged EXEC)</td>
<td>Displays the Ports slot/port</td>
</tr>
<tr>
<td></td>
<td>Type - Indicates if the port is a special type of port</td>
</tr>
<tr>
<td></td>
<td>Admin Mode - Selects the Port Control Administration State</td>
</tr>
<tr>
<td></td>
<td>Physical Mode - Selects the desired port speed and duplex mode</td>
</tr>
<tr>
<td></td>
<td>Physical Status - Indicates the port speed and duplex mode</td>
</tr>
<tr>
<td></td>
<td>Link Status - Indicates whether the link is up or down</td>
</tr>
<tr>
<td></td>
<td>Link Trap - Determines whether or not to send a trap when link status changes</td>
</tr>
</tbody>
</table>

*Table 1: Quick Start up Physical Port Data*

■ Quick Start up User Account Management

<table>
<thead>
<tr>
<th>Command</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>show users (in Privileged EXEC)</td>
<td>Displays all of the users that are allowed to access the switch</td>
</tr>
<tr>
<td></td>
<td>Access Mode - Shows whether the user is able to change parameters on the switch(Read/Write) or is only able to view them (Read Only).</td>
</tr>
<tr>
<td></td>
<td>As a factory default, the ‘admin’ user has Read/Write access and the ‘user’ user has Read Only access. There can only be one Read/Write user and up to five Read Only users.</td>
</tr>
</tbody>
</table>

| show loginsession (in User EXEC) | Displays all of the login session information |

*Table 2: Quick Start up User Account Management*
### Quick Start up User Account Management

<table>
<thead>
<tr>
<th>Command</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>users passwd &lt;username&gt;</strong>&lt;br&gt;(in Global Config)</td>
<td>Allows the user to set passwords or change passwords needed to login&lt;br&gt;A prompt will appear after the command is entered requesting the users old password. In the absence of an old password leave the area blank. The operator must press enter to execute the command.&lt;br&gt;The system then prompts the user for a new password then a prompt to confirm the new password. If the new password and the confirmed password match a message will be displayed. &lt;br&gt;User password should not be more than eight characters in length. &lt;br&gt;Make sure, that the passwords of the users differ from each other. If two or more users try to choose the same password, the CLI will display an error message.</td>
</tr>
<tr>
<td><strong>copy system:running-config nvram:startup-config</strong>&lt;br&gt;(in Privileged EXEC)</td>
<td>This will save passwords and all other changes to the device.&lt;br&gt;If you do not save the configuration by doing this command, all configurations will be lost when a power cycle is performed on the switch or when the switch is reset.</td>
</tr>
<tr>
<td><strong>logout</strong>&lt;br&gt;(in User EXEC and Privileged EXEC)</td>
<td>Logs the user out of the switch</td>
</tr>
</tbody>
</table>

*Table 2: Quick Start up User Account Management*
Quick Start up IP Address

To view the network parameters the operator can access the device by the following two methods.

- Simple Network Management Protocol - SNMP
- Web Browser

Note: Helpful Hint: The user should do a ‘copy system:running-config nvram:startup-config’ after configuring the network parameters so that the configurations are not lost.

<table>
<thead>
<tr>
<th>Command</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>show network</td>
<td>Displays the Network Configurations</td>
</tr>
<tr>
<td>(in User EXEC)</td>
<td></td>
</tr>
<tr>
<td>network parms</td>
<td>Sets the IP Address, subnet mask and gateway of the router. The IP Address and the gateway must be on the same subnet.</td>
</tr>
<tr>
<td>&lt;ipaddr&gt; &lt;net-mask&gt; [gateway]</td>
<td>(in Privileged EXEC)</td>
</tr>
</tbody>
</table>

IP Address range from 0.0.0.0 to 255.255.255.255
Subnet Mask range from 0.0.0.0 to 255.255.255.255
Gateway Address range from 0.0.0.0 to 255.255.255.255

Table 3: Quick Start up IP Address
Quick Start up Downloading from TFTP Server
Before starting a TFTP server download, the operator must complete the Quick Start up for the IP Address.

<table>
<thead>
<tr>
<th>Command</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>`copy &lt;url&gt; {nvram:startup-config</td>
<td>system:image}`</td>
</tr>
</tbody>
</table>

Table 4: Quick Start up Downloading from TFTP Server

Quick Start up Factory Defaults

<table>
<thead>
<tr>
<th>Command</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>clear config</code> (in Privileged EXEC Mode)</td>
<td>Enter yes when the prompt pops up to clear all the configurations made to the switch.</td>
</tr>
<tr>
<td><code>copy system:running-config nvram:startup-config</code></td>
<td>Enter yes when the prompt pops up that asks if you want to save the configurations made to the switch.</td>
</tr>
<tr>
<td><code>reboot</code> (or cold boot the switch) (in Privileged EXEC Mode)</td>
<td>Enter yes when the prompt pops up that asks if you want to reset the system. This is the users choice either reset the switch or cold boot the switch, both work effectively.</td>
</tr>
</tbody>
</table>

Table 5: Quick Start up Factory Defaults
1 Command Structure

The Command Line Interface (CLI) syntax, conventions and terminology are described in this section. Each CLI command is illustrated using the structure outlined below.
1.1 Format

Commands are followed by values, parameters, or both.

**Example 1**

```
network parms <ipaddr> <netmask> [gateway]
```

- `network parms` is the command name.
- `<ipaddr> <netmask>` are the required values for the command.
- `[gateway]` is the optional value for the command.

**Example 2**

```
snmp-server location <loc>
```

- `snmp-server location` is the command name.
- `<loc>` is the required parameter for the command.

**Example 3**

```
clear config
```

- `clear config` is the command name.

1.1.1 Command

The text in courier font is to be typed exactly as shown.
1.1.2 Parameters

Parameters are order dependent.

Parameters are displayed in this document in italic font, which are to be replaced with a name or number.

To use spaces as part of parameter name, enclose it in double quotes. For example, the expression "System Name with Spaces" forces the system to accept the spaces.

Parameters may be mandatory values, optional values, choices, or a combination.

- `<parameter>`. The <> angle brackets indicate that a mandatory parameter is to be entered in place of the brackets and text inside them.
- `[parameter]`. The [] square brackets indicate that an optional parameter may be entered in place of the brackets and text inside them.
- `choice1 | choice2`. The | indicates that only one of the parameters should be entered.
- The {} curly braces indicate that a parameter must be chosen from the list of choices.

1.1.3 Values

**ipaddr**

This parameter is a valid IP address. Presently the IP address can be entered in following formats:

- `a` (32 bits)
- `a.b` (8.24 bits)
- `a.b.c` (8.8.16 bits)
- `a.b.c.d` (8.8.8.8 bits)

In addition to these formats, decimal, hexadecimal and octal formats are supported through the following input formats (where n is any valid hexadecimal, octal or decimal number):

- `0xn` (CLI assumes hexadecimal format)
0n (CLI assumes octal format with leading zeros)
n (CLI assumes decimal format)

**macaddr**
The MAC address format is six hexadecimal numbers separated by colons, for example 00:06:29:32:81:40.

**areaid**
Area IDs may be entered in dotted-decimal notation (for example, 0.0.0.1). An area ID of 0.0.0.0 is reserved for the backbone. Area IDs have the same form as IP addresses, but are distinct from IP addresses. The IP network address of the sub-netted network may be used for the area ID.

**slot/port**
Valid slot and port number separated by forward slashes. For example, 1/1 represents slot number 1 and port number 1.

**logical slot/port**
Logical slot and port number. This is applicable in the case of a link-aggregation (LAG) and vlan router interfaces (9/x). The operator can use the logical slot/port to configure the link-aggregation.

**routerid**
The value of <router id> must be entered in 4-digit dotted-decimal notation (for example, 0.0.0.1). A router ID of 0.0.0.0 is invalid.

**Interface**
Valid slot and port number separated by forward slashes. For example, 0/1 represents slot number 0 and port number 1.

**Logical Interface**
Logical slot and port number. This is applicable in the case of a port-channel (LAG) and vlan router interfaces (9/x). The operator can use the logical slot/port to configure the port-channel.

**Character strings**
Use double quotation marks to identify character strings, for example, “System Name with Spaces”. An empty string (“”) is not valid.
1.1.4 Conventions

Network addresses are used to define a link to a remote host, workstation or network. Network addresses are shown using the following syntax:

<table>
<thead>
<tr>
<th>Address Type</th>
<th>Format</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipaddr</td>
<td>192.168.11.110</td>
<td>0.0.0.0 to 255.255.255.255 (decimal)</td>
</tr>
<tr>
<td>macaddr</td>
<td>A7:C9:89:DD:A9:B3</td>
<td>hexadecimal digit pairs</td>
</tr>
</tbody>
</table>

Table 1: Network Address Syntax

Double quotation marks such as "System Name with Spaces" set off user defined strings. If the operator wishes to use spaces as part of a name parameter then it must be enclosed in double quotation marks.

Empty strings ("") are not valid user defined strings.

Command completion finishes spelling the command when enough letters of a command are typed to uniquely identify the command word. The command may be executed by typing <enter> (command abbreviation) or the command word may be completed by typing the <tab> or <space bar> (command completion).

The value 'Err' designates that the requested value was not internally accessible.

The value '-----' designates that the value is unknown.
1.1.5 Annotations

The CLI allows the user to type single-line annotations at the command prompt for use when writing test or configuration scripts and for better readability. The exclamation point (‘!’) character flags the beginning of a comment. The comment flag character can begin a word anywhere on the command line and all input following this character is ignored. Any command line that begins with the character ‘!’ is recognized as a comment line and ignored by the parser.

Some examples are provided below:

```plaintext
! Script file for setting the CLI prompt
set prompt example-switch
! End of the script file
```
1.1.6 Special keys

The following list of special keys may be helpful to enter command lines.

BS       delete previous character
Ctrl-A   go to beginning of line
Ctrl-E   go to end of line
Ctrl-F   go forward one character
Ctrl-B   go backward one character
Ctrl-D   delete current character
Ctrl-H   display command history or retrieve a command
Ctrl-U, X delete to beginning of line
Ctrl-K   delete to end of line
Ctrl-W   delete previous word
Ctrl-T   transpose previous character
Ctrl-P   go to previous line in history buffer
Ctrl-R   rewrites or pastes the line
Ctrl-N   go to next line in history buffer
Ctrl-Y   print last deleted character
Ctrl-Q   enables serial flow
Ctrl-S   disables serial flow
Ctrl-Z   return to root command prompt
Tab, <SPACE> command-line completion
Exit     go to next lower command prompt
?        list choices

Note:
2 Mode-based CLI

The CLI groups all the commands in appropriate modes according to the nature of the command. A sample of the CLI command modes are described below. Each of the command modes support specific software commands.

- User Exec Mode
- Privileged Exec Mode
- Global Config Mode
- Interface Config Mode
- Line Config Mode

The Command Mode table captures the command modes, the prompts visible in that mode and the exit method from that mode.

<table>
<thead>
<tr>
<th>Command Mode</th>
<th>Access Method</th>
<th>Prompt</th>
<th>Exit or Access Next Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Exec Mode</td>
<td>This is the first level of access. Perform basic tasks and list system info</td>
<td>(Hirschmann Product) &gt;</td>
<td>Enter Logout command</td>
</tr>
<tr>
<td>Privileged Exec Mode</td>
<td>From the User Exec Mode, enter the enable command</td>
<td>(Hirschmann Product) #</td>
<td>To exit to the User Exec mode, enter exit or press Ctrl-Z.</td>
</tr>
<tr>
<td>Global Config Mode</td>
<td>From the Privileged Exec mode, enter the configure command</td>
<td>(Hirschmann Product) (Config) #</td>
<td>To exit to the Privileged Exec mode, enter the exit command, or press Ctrl-Z to switch to user exec mode.</td>
</tr>
<tr>
<td>Interface Config Mode</td>
<td>From the Global Configuration mode, enter the interface &lt;slot/port&gt; command</td>
<td>(Hirschmann Product) (Interface-&quot;if number&quot;) #</td>
<td>To exit to the Global Config mode enter exit. To return to user EXEC mode enter ctrl-Z.</td>
</tr>
<tr>
<td>Line Config Mode</td>
<td>From the Global Configuration mode, enter the lineconfig command</td>
<td>(Hirschmann Product) (line) #</td>
<td>To exit to the Global Config mode enter exit. To return to User Exec mode enter ctrl-Z.</td>
</tr>
</tbody>
</table>

Table 3: Command Mode
2.1 Mode-based Topology

The CLI tree is built on a mode concept where the commands are available according to the interface. Some of the modes are depicted in the following figure.

Fig. 1: Mode-based CLI
2.2 Mode-based Command Hierarchy

The CLI is divided into various modes. The Commands in one mode are not available until the operator switches to that particular mode, with the exception of the User Exec mode commands. The User Exec mode commands may also be executed in the Privileged Exec mode. The commands available to the operator at any point in time depend upon the mode. Entering a question mark (?) at the CLI prompt, displays a list of the available commands and descriptions of the commands.

The CLI provides the following modes:

User Exec Mode
When the operator logs into the CLI, the User Exec mode is the initial mode. The User Exec mode contains a limited set of commands. The command prompt shown at this level is:
Command Prompt: (Hirschmann Product)>

Privileged Exec Mode
To have access to the full suite of commands, the operator must enter the Privileged Exec mode. Privileged users authenticated by login are able to enter the Privileged EXEC mode. From Privileged Exec mode, the operator can issue any Exec command, enter the Global Configuration mode. The command prompt shown at this level is:
Command Prompt: (Hirschmann Product)#

Global Config Mode
This mode permits the operator to make modifications to the running configuration. General setup commands are grouped in this mode. From the Global Configuration mode, the operator can enter the System Configuration mode, the Physical Port Configuration mode, the Interface Configuration mode, or the Protocol Specific modes specified below. The command prompt at this level is:
Command Prompt: (Hirschmann Product)(Config)#

From the Global Config mode, the operator may enter the following configuration modes:
2.2 Mode-based Command Hierarchy

Interface Config Mode

Many features are enabled for a particular interface. The Interface commands enable or modify the operation of an interface.

In this mode, a physical port is set up for a specific logical connection operation. The Interface Config mode provides access to the router interface configuration commands. The command prompt at this level is:

Command Prompt: (Hirschmann Product)(Interface <slot/port>)#

The resulting prompt for the interface configuration command entered in the Global Configuration mode is shown below:

(Hirschmann Product)(Config)# interface 2/1
(Hirschmann Product)(Interface 2/1)#

Line Config Mode

This mode allows the operator to configure the console interface. The operator may configure the interface from the directly connected console. The command prompt at this level is:

Command Prompt: (Hirschmann Product)(Line)#

MAC Access-List Config Mode

Use the MAC Access-List Config mode to create a MAC Access-List and to enter the mode containing Mac Access-List configuration commands.

(Hirschmann Product)(Config)# mac-access-list extended <name>
Command Prompt: (Hirschmann Product)(Config mac-access-list)#
2.3 Flow of Operation

This section captures the flow of operation for the CLI:

- The operator logs into the CLI session and enters the User Exec mode. In the User Exec mode the (Hirschmann Product) (exec)> prompt is displayed on the screen.

The parsing process is initiated whenever the operator types a command and presses <ENTER>. The command tree is searched for the command of interest. If the command is not found, the output message indicates where the offending entry begins. For instance, command node A has the command "show spanning-tree" but the operator attempts to execute the command "show arpp brief" then the output message would be (Hirschmann Product) (exec)> show sspanning-tree^.

%Invalid input detected at '^' marker.

If the operator has given an invalid input parameter in the command, then the message conveys to the operator an invalid input was detected. The layout of the output is depicted below:

(Hirschmann Product) (exec) #show sspanning-tree

^  
(Hirschmann Product) Invalid input detected at '^' marker.

Fig. 2: Syntax Error Message

After all the mandatory parameters are entered, any additional parameters entered are treated as optional parameters. If any of the parameters are not recognized a syntax error message will be displayed.

- After the command is successfully parsed and validated, the control of execution goes to the corresponding CLI callback function.
For mandatory parameters, the command tree extends till the mandatory parameters make the leaf of the branch. The callback function is only invoked when all the mandatory parameters are provided. For optional parameters, the command tree extends till the mandatory parameters and the optional parameters make the leaf of the branch. However, the callback function is associated with the node where the mandatory parameters are fetched. The callback function then takes care of the optional parameters.

Once the control has reached the callback function, the callback function has complete information about the parameters entered by the operator.
2.4 “No” Form of a Command

“No” is a specific form of an existing command and does not represent a new or distinct command. Only the configuration commands are available in the “no” form. The behavior and the support details of the “no” form is captured as part of the mapping sheets.

2.4.1 Support for “No” Form

Almost every configuration command has a “no” form. In general, use the no form to reverse the action of a command or reset a value back to the default. For example, the no shutdown interface configuration command reverses the shutdown of an interface. Use the command without the keyword "no" to re-enable a disabled feature or to enable a feature that is disabled by default.

2.4.2 Behavior of Command Help ("?")

The “no” form is treated as a specific form of an existing command and does not represent a new or distinct command. However, the behavior of the “?” and help text differ for the “no” form (the help message shows only options that apply to the “no” form).

- The help message is the same for all forms of the command. The help string may be augmented with details about the “no” form behavior.

- For the (no interface?) and (no inte?) cases of the “?”, the options displayed are identical to the case when the “no” token is not specified as in (interface) and (inte?).
3 CLI Commands: Base

This chapter provides detailed explanation of the Switching commands. The commands are divided into five functional groups:

- Show commands display switch settings, statistics, and other information.
- Configuration commands configure features and options of the switch. For every configuration command, there is a show command that displays the configuration setting.
- Copy commands transfer or save configuration and informational files to and from the switch.
- Clear commands clear
  - some (e.g. the "clear arp-table-switch" command which clears the agent’s ARP table) or
  - all (e.g. the "clear config" command which resets the whole configuration to the factory defaults)

This chapter includes the following configuration types:

- System information and statistics commands
- Management commands
- Device configuration commands
- User account management commands
- Security commands
- System utilities
- Link Layer Discovery Protocol Commands
- Simple Network Time Protocol Commands
- Precision Time Protocol Commands
- Power over Ethernet Commands
3.1 System Information and Statistics Commands

3.1.1 show arp switch
This command displays the Address Resolution Protocol cache of the switch.

Format
   show arp switch

Mode
   Privileged EXEC and User EXEC

3.1.2 show bridge aging-time
This command displays the timeout for address aging.

Format
   show bridge aging-time

Mode
   Privileged EXEC and User EXEC
3.1.3  show bridge fast-link-detection

This command displays the Bridge Fast Link Detection setting.

**Format**

```
show bridge fast-link-detection
```

**Mode**

Privileged EXEC and User EXEC

---

3.1.4  show config-watchdog

Activating the watchdog enables you to return automatically to the last configuration after a set time period has elapsed. This gives you back your access to the Switch.

**Format**

```
show config-watchdog
```

**Mode**

Privileged EXEC and User EXEC
### 3.1.5 show device-status

The signal device status is for displaying

- the monitoring functions of the switch,
- the device status trap setting.

**Format**

```
show device-status
[monitor|state|trap]
```

**Mode**

Privileged EXEC and User EXEC

**Device status monitor**

Displays the possible monitored events and which of them are monitored:

- the detected failure of at least one of the supply voltages.
- the removal of the ACA
- the removal of a media module
- the temperature limits
- the defective link status of at least one port. With the switch, the indication of link status can be masked by the management for each port. Link status is not monitored in the delivery condition.
- the loss of Redundancy guarantee.

**Device status state**

- **Error** The current device status is error.
- **No Error** The current device status is no error.

**Device status trap**

- **enabled** A trap is sent if the device status changes.
- **disabled** No trap is sent if the device status changes.
### 3.1.6 show eventlog

This command displays the event log, which contains error messages from the system. The event log is not cleared on a system reset.

**Format**

`show eventlog`

**Mode**

Privileged EXEC and User EXEC

**File**

The file in which the event originated.

**Line**

The line number of the event

**Task Id**

The task ID of the event.

**Code**

The event code.

**Time**

The time this event occurred.

**Note:** Event log information is retained across a switch reset.
3.1.7 show interface

This command displays a summary of statistics for a specific port or a count of all CPU traffic based upon the argument.

**Format**

```
show interface {<slot/port> | ethernet{<slot/port>|switchport} | switchport}
```

**Mode**

Privileged EXEC and User EXEC

The display parameters, when the argument is '<slot/port>', is as follows:

**Packets Received Without Error**
The total number of packets (including broadcast packets and multicast packets) received by the processor.

**Packets Received With Error**
The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.

**Broadcast Packets Received**
The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.

**Packets Transmitted Without Error**
The total number of packets transmitted out of the interface.

**Transmit Packets Errors**
The number of outbound packets that could not be transmitted because of errors.

**Collisions Frames**
The best estimate of the total number of collisions on this Ethernet segment.

**Time Since Counters Last Cleared**
The elapsed time, in days, hours, minutes, and seconds since the statistics for this port were last cleared.

The display parameters, when the argument is 'switchport', is as follows:
Packets Received Without Error
The total number of packets (including broadcast packets and multicast packets) received by the processor.

Broadcast Packets Received
The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.

Packets Received With Error
The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.

Packets Transmitted Without Error
The total number of packets transmitted out of the interface.

Broadcast Packets Transmitted
The total number of packets that higher-level protocols requested to be transmitted to the Broadcast address, including those that were discarded or not sent.

Transmit Packet Errors
The number of outbound packets that could not be transmitted because of errors.

Address Entries Currently In Use
The total number of Forwarding Database Address Table entries now active on the switch, including learned and static entries.

Time Since Counters Last Cleared
The elapsed time, in days, hours, minutes, and seconds since the statistics for this switch were last cleared.
### 3.1.8 show interface ethernet

This command displays detailed statistics for a specific port or for all CPU traffic based upon the argument.

**Format**

```
show interface ethernet {<slot/port> | switchport}
```

**Mode**

Privileged EXEC and User EXEC

The display parameters, when the argument is '<slot/port>', are as follows:

**Packets Received**

- **Octets Received** - The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including Frame Check Sequence (FCS) octets). This object can be used as a reasonable estimate of ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval. The result of this equation is the value Utilization which is the percent utilization of the ethernet segment on a scale of 0 to 100 percent.

- **Packets Received < 64 Octets** - The total number of packets (including bad packets) received that were < 64 octets in length (excluding framing bits but including FCS octets).

- **Packets Received 64 Octets** - The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).

- **Packets Received 65-127 Octets** - The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).

- **Packets Received 128-255 Octets** - The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).

- **Packets Received 256-511 Octets** - The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).

- **Packets Received 512-1023 Octets** - The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
octets in length inclusive (excluding framing bits but including FCS octets).

**Packets Received 1024-1518 Octets** - The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).

**Packets Received 1519-1522 Octets** - The total number of packets (including bad packets) received that were between 1519 and 1522 octets in length inclusive (excluding framing bits but including FCS octets).

**Packets Received > 1522 Octets** - The total number of packets received that were longer than 1522 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.

**Packets Received Successfully**

- **Total** - The total number of packets received that were without errors.

- **Unicast Packets Received** - The number of subnetwork-unicast packets delivered to a higher-layer protocol.

- **Multicast Packets Received** - The total number of good packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.

- **Broadcast Packets Received** - The total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets.

**Packets Received with MAC Errors**

- **Total** - The total number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.

- **Jabbers Received** - The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). Note that this definition of jabber is different than the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define jabber as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms.

- **Fragments/Undersize Received** - The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets).
Alignment Errors - The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with a non-integral number of octets.

Rx FCS Errors - The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with an integral number of octets.

Overruns - The total number of frames discarded as this port was overloaded with incoming packets, and could not keep up with the inflow.

Received Packets not forwarded

Total - A count of valid frames received which were discarded (i.e. filtered) by the forwarding process.

Local Traffic Frames - The total number of frames dropped in the forwarding process because the destination address was located off of this port.

802.3x Pause Frames Received - A count of MAC Control frames received on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode.

Unacceptable Frame Type - The number of frames discarded from this port due to being an unacceptable frame type.

Reserved Address Discards - The number of frames discarded that are destined to an IEEE 802.1 reserved address and are not supported by the system.

Broadcast Storm Recovery - The number of frames discarded that are destined for FF:FF:FF:FF:FF:FF when Broadcast Storm Recovery is enabled.

CFI Discards - The number of frames discarded that have CFI bit set and the addresses in RIF are in non-canonical format.

Upstream Threshold - The number of frames discarded due to lack of cell descriptors available for that packet's priority level.

Packets Transmitted Octets

Total Bytes - The total number of octets of data (including those in bad packets) transmitted into the network (excluding framing bits but including FCS octets). This object can be used as a reasonable estimate of ethernet utilization. If greater precision is desired, the ether-
StatsPkts and etherStatsOctets objects should be sampled before and after a common interval. -----

**Packets Transmitted 64 Octets** - The total number of packets (including bad packets) transmitted that were 64 octets in length (excluding framing bits but including FCS octets).

**Packets Transmitted 65-127 Octets** - The total number of packets (including bad packets) transmitted that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).

**Packets Transmitted 128-255 Octets** - The total number of packets (including bad packets) transmitted that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).

**Packets Transmitted 256-511 Octets** - The total number of packets (including bad packets) transmitted that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).

**Packets Transmitted 512-1023 Octets** - The total number of packets (including bad packets) transmitted that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).

**Packets Transmitted 1024-1518 Octets** - The total number of packets (including bad packets) transmitted that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).

**Packets Transmitted 1519-1522 Octets** - The total number of packets (including bad packets) transmitted that were between 1519 and 1522 octets in length inclusive (excluding framing bits but including FCS octets).

**Max Info** - The maximum size of the Info (non-MAC) field that this port will receive or transmit.

**Packets Transmitted Successfully**

- **Total** - The number of frames that have been transmitted by this port to its segment.

- **Unicast Packets Transmitted** - The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.

- **Multicast Packets Transmitted** - The total number of packets that higher-level protocols requested be transmitted to a Multicast address, including those that were discarded or not sent.
Broadcast Packets Transmitted - The total number of packets that higher-level protocols requested be transmitted to the Broadcast address, including those that were discarded or not sent.

Transmit Errors
Total Errors - The sum of Single, Multiple, and Excessive Collisions.
Tx FCS Errors - The total number of packets transmitted that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with an integral number of octets
Oversized - The total number of frames that exceeded the max permitted frame size. This counter has a max increment rate of 815 counts per sec. at 10 Mb/s.
Underrun Errors - The total number of frames discarded because the transmit FIFO buffer became empty during frame transmission.

Transmit Discards
Total Discards - The sum of single collision frames discarded, multiple collision frames discarded, and excessive frames discarded.
Single Collision Frames - A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision.
Multiple Collision Frames - A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision.
Excessive Collisions - A count of frames for which transmission on a particular interface is discontinued due to excessive collisions.
Port Membership - The number of frames discarded on egress for this port due to egress filtering being enabled.

Protocol Statistics
BPDUs received - The count of BPDUs (Bridge Protocol Data Units) received in the spanning tree layer.
BPDUs Transmitted - The count of BPDUs (Bridge Protocol Data Units) transmitted from the spanning tree layer.
802.3x Pause Frames Received - A count of MAC Control frames received on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode.
GVRP PDU's Received - The count of GVRP PDU's received in the GARP layer.
STP BPDU Transmitted - Spanning Tree Protocol Bridge Protocol Data Units sent
STP BPDU Received - Spanning Tree Protocol Bridge Protocol Data Units received
RST BPDU Transmitted - Rapid Spanning Tree Protocol Bridge Protocol Data Units sent
RSTP BPDU Received - Rapid Spanning Tree Protocol Bridge Protocol Data Units received
MSTP BPDU Transmitted - Multiple Spanning Tree Protocol Bridge Protocol Data Units sent
MSTP BPDU Received - Multiple Spanning Tree Protocol Bridge Protocol Data Units received

Time Since Counters Last Cleared
The elapsed time, in days, hours, minutes, and seconds since the statistics for this port were last cleared.

The display parameters, when the argument is 'switchport, are as follows:
Octets Received - The total number of octets of data received by the processor (excluding framing bits but including FCS octets).
Total Packets Received Without Error - The total number of packets (including broadcast packets and multicast packets) received by the processor.
Unicast Packets Received - The number of subnetwork-unicast packets delivered to a higher-layer protocol.
Multicast Packets Received - The total number of packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.
Broadcast Packets Received - The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Receive Packets Discarded - The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.
Octets Transmitted - The total number of octets transmitted out of the interface, including framing characters.
**Packets Transmitted without Errors** - The total number of packets transmitted out of the interface.

**Unicast Packets Transmitted** - The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.

**Multicast Packets Transmitted** - The total number of packets that higher-level protocols requested be transmitted to a Multicast address, including those that were discarded or not sent.

**Broadcast Packets Transmitted** - The total number of packets that higher-level protocols requested be transmitted to the Broadcast address, including those that were discarded or not sent.

**Transmit Packets Discarded** - The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.

**Most Address Entries Ever Used** - The highest number of Forwarding Database Address Table entries that have been learned by this switch since the most recent reboot.

**Address Entries in Use** - The number of Learned and static entries in the Forwarding Database Address Table for this switch.

**Time Since Counters Last Cleared**

The elapsed time, in days, hours, minutes, and seconds, since the statistics for this switch were last cleared.
3.1.9  show interface switchport

This command displays data concerning the internal port to the management agent.

**Format**

```
show interface switchport
```

**Mode**

Privileged EXEC and User EXEC

3.1.10 show logging

This command displays the trap log maintained by the switch. The trap log contains a maximum of 256 entries that wrap.

**Format**

```
show logging [buffered | hosts | traplogs | snmp-requests]
```

**Mode**

Privileged EXEC and User EXEC

**buffered**

Display buffered (in-memory) log entries.

**hosts**

Display logging hosts.

**traplogs**

Display trap records.

**snmp-requests**

Display logging SNMP requests and severity level.
3.1.11 show mac-addr-table

This command displays the forwarding database entries. If the command is entered with no parameter, the entire table is displayed. This is the same as entering the optional *all* parameter. Alternatively, the administrator can enter a MAC Address to display the table entry for the requested MAC address and all entries following the requested MAC address.

**Note:** This command displays only learned unicast addresses. For other addresses use the command show mac-filter-table.

**Format**

```
show mac-addr-table [<macaddr> <1-4042> | all]
```

**Mode**

Privileged EXEC and User EXEC

**Mac Address**

A unicast MAC address for which the switch has forwarding and or filtering information. The format is 6 or 8 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB.

**Slot/Port**

The port which this address was learned.

**if Index**

This object indicates the ifIndex of the interface table entry associated with this port.

**Status**

The status of this entry. The meanings of the values are:

- **Learned** The value of the corresponding instance was learned by observing the source MAC addresses of incoming traffic, and is currently in use.
- **Management** The value of the corresponding instance (system MAC address) is also the value of an existing instance of dot1dStaticAddress.
3.1.12 show signal-contact

The signal contact is for displaying

- the manual setting and the current state of the signal contact,
- the monitoring functions of the switch,
- the signal-contacts trap setting.

**Format**

```
show signal-contact
[1|2|all [mode|monitor|state|trap]]
```

**Mode**

Privileged EXEC and User EXEC

**Signal contact mode**

Auto The signal contact monitors the functions of the switch which makes it possible to perform remote diagnostics.

A break in contact is reported via the zero-potential signal contact (relay contact, closed circuit).

Device Status The signal contact monitors the device-status.

Manual This command gives you the option of remote switching the signal contact.

**Signal contact monitor**

Displays the possible monitored events and which of them are monitored:

- the detected failure of at least one of the supply voltages.
- the removal of the ACA
- the removal of a media module
- the temperature limits
- the defective link status of at least one port. With the switch, the indication of link status can be masked by the management for each port. Link status is not monitored in the delivery condition.
- the loss of Redundancy guarantee.

**Signal contact manual setting**

closed The signal contact’s manual setting is closed.

open The signal contact’s manual setting is open.

**Signal contact operating state**

closed The signal contact is currently closed.

open The signal contact is currently open.
Signal contact trap
   enabled A trap is sent if the signal contact state changes.
   disabled No trap is sent if the signal contact state changes.

Note: To show the signal contact's port related settings, use the command show port {<slot/port> | all} (see “show port” on page 126).

3.1.13 show slot

This command is used to display information about slot(s).
For [slot] enter the slot ID.

Format
   show slot [slot]

Mode
   Privileged EXEC
3.1.14 show running-config

This command is used to display the current setting of different protocol packages supported on the switch. This command displays only those parameters, the values of which differ from default value. The output is displayed in the script format, which can be used to configure another switch with the same configuration.

Format

show running-config [all]

Mode

Privileged EXEC

all

Show all the running configuration on the switch. All configuration parameters will be output even if their value is the default value.

3.1.15 show sysinfo

This command displays switch information.

Format

show sysinfo

Mode

Privileged EXEC and User EXEC

Alarm

Displays the latest present Alarm for a signal contact.

System Description

Text used to identify this switch.

System Name

Name used to identify the switch.

System Location

Text used to identify the location of the switch. May be up to 31 alphanumeric characters. The factory default is blank.
System Contact
   Text used to identify a contact person for this switch. May be up to 31 alpha-numeric characters. The factory default is blank.

System UpTime
   The time in days, hours and minutes since the last switch reboot.

System Date and Time
   The system clock´s date and time in local time zone.

System IP Address
   The system´s IP address.

Boot Software Release
   The boot code´s version number.

Boot Software Build Date
   The boot code´s build date.

Operating system Software Release
   The operating system´s software version number.

Operating system Software Build Date
   The operating system´s software build date.

Backplane Hardware Revision
   The hardware´s revision number.

Backplane Hardware Description
   The hardware´s device description.

Serial Number (Backplane)
   The hardware´s serial number.

Base MAC Address (Backplane)
   The hardware´s base MAC address.

Number of MAC Addresses (Backplane)
   The number of hardware MAC addresses.

Configuration state
   The state of the actual configuration.

Auto Config Adapter, State
   The Auto Configuration Adapter's state.
Auto Config Adapter, Serial Number
The Auto Configuration Adapter's serial number (if present and operative).

Power Supply Information
The status of the power supplies.

Media Module Information
The description of each media module
Note: Media Module information is available exclusively on devices equipped with media modules.
SFP specific information is available exclusively on devices equipped with SFP modules.
– Description: media module type,
– Serial Number of the media module (if available),
– SFP Part ID: SFP type (if available),
– SFP Serial No. of the SFP module (if available),
– SFP Supported: yes/no,
– SFP Temperature (°C, F),
– SFP Tx Pwr, SFP transmit power (mW),
– SFP Rx Pwr, SFP receive power (mW),
– SFP Rx Pwr State: ok/warning/alarm.

CPU Utilization
The utilization of the central processing unit.

Flashdisk
Free memory on flashdisk (in Kbytes).
This chapter provides a detailed explanation of the QoS CoS commands. The following commands are available.

The commands are divided into these different groups:

- Configuration Commands are used to configure features and options of the switch. For every configuration command there is a show command that will display the configuration setting.

- Show commands are used to display device settings, statistics and other information.

Note: The 'Interface Config' mode only affects a single interface, whereas the 'Global Config' mode is applied to all interfaces.
3.2.1 classofservice dot1p-mapping

This command maps an 802.1p priority to an internal traffic class for a device when in ‘Global Config’ mode. The number of available traffic classes may vary with the platform. Userpriority and trafficclass can both be the range from 0-7. The command is only available on platforms that support priority to traffic class mapping on a ‘per-port’ basis, and the number of available traffic classes may vary with the platform.

**Format**

```
classofservice dot1p-mapping
    <userpriority> <trafficclass>
```

**Mode**

Global Config or Interface Config

**userpriority**

Enter the 802.1p priority (0-7).

**trafficclass**

Enter the traffic class to map the 802.1p priority (0-3).

---

**no classofservice dot1p-mapping**

This command restores the default mapping of the 802.1p priority to an internal traffic class.

**Format**

```
no classofservice dot1p-mapping
```

**Modes**

Global Config or Interface Config
### 3.2.2 classofservice ip-dscp-mapping

This command maps an IP DSCP value to an internal traffic class. The `<ipdscp>` value is specified as either an integer from 0 to 63, or symbolically through one of the following keywords: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef.

**Format**

```
classofservice ip-dscp-mapping
   <ipdscp> <trafficclass>
```

**Mode**

Global Config

**ipdscp**

Enter the IP DSCP value in the range of 0 to 63 or an IP DSCP keyword (af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef).

**trafficclass**

Enter the traffic class to map the 802.1p priority (0-3).

---

#### no classofservice ip-dscp-mapping

This command restores the default mapping of the IP DSCP value to an internal traffic class.

**Format**

```
no classofservice dot1p-mapping
```

**Modes**

Global Config
3.2.3 classofservice trust

This command sets the class of service trust mode of an interface. The mode can be set to trust one of the Dot1p (802.1p) or IP DSCP packet markings.

**Note:** In trust ip-dscp mode the switch modifies the vlan priority for outgoing frames according to
– the a fix mapping table
(see Reference Manual "Web-based Management" for further details).

**Format**
```
 classofservice trust dot1p | ip-dscp
```

**Mode**
- Global Config

**no classofservice trust**

This command sets the interface mode to untrusted, i.e. the packet priority marking is ignored and the default port priority is used instead.

**Format**
```
 no classofservice trust
```

**Modes**
- Global Config
3.2.4  show classofservice dot1p-mapping

This command displays the current 802.1p priority mapping to internal traffic classes for a specific interface. The slot/port parameter is required on platforms that support priority to traffic class mapping on a 'per-port' basis.

Platforms that support priority to traffic class mapping on a per-port basis:

**Format**

```
show classofservice dot1p-mapping
```

Platforms that do not support priority to traffic class mapping on a per-port basis:

**Format**

```
show classofservice dot1p-mapping
```

**Mode**

Privileged EXEC and User EXEC
3.2.5  show classofservice ip-dscp-mapping

This command displays the current IP DSCP mapping to internal traffic classes for the global configuration settings.

Format

    show classofservice ip-dscp-mapping [<slot/port>]

Mode

    Privileged EXEC

The following information is repeated for each user priority.

**IP DSCP**

    The IP DSCP value.

**Traffic Class**

    The traffic class internal queue identifier to which the IP DSCP value is mapped.

**slot/port**

    Valid slot and port number separated by forward slashes.
3.2.6 **show classofservice trust**

This command displays the current trust mode for the specified interface. The slot/port parameter is optional. If specified, the trust mode of the interface is displayed. If omitted, the most recent global configuration settings are displayed.

**Format**

```
show classofservice trust [slot/port]
```

**Mode**

Privileged EXEC

**Class of Service Trust Mode**

The current trust mode: Dot1p, IP DSCP, or Untrusted.

**Untrusted Traffic Class**

The traffic class used for all untrusted traffic. This is only displayed when the COS trust mode is set to 'untrusted'.

**slot/port**

Valid slot and port number separated by forward slashes.
3.3 Management Commands

These commands manage the switch and show current management settings.

3.3.1 bridge aging-time

This command configures the forwarding database address aging timeout in seconds.

Default
30

Format
bridge aging-time <15-3825>

Mode
Global Config

Seconds
The <seconds> parameter must be within the range of 15 to 3825 seconds.

no bridge aging-time

This command sets the forwarding database address aging timeout to 30 seconds.

Format
no bridge aging-time

Mode
Global Config
3.3.2 bridge fast-link-detection

This command enables or disables the Bridge Fast Link Detection.

Default
   Enabled

Format
   bridge fast-link-detection {disable|enable}

Mode
   Global Config

3.3.3 network javascriptmode

When the user accesses the switch’s web interface, the switch’s web server will deliver a HTML page that contains JavaScript.

Default
   enabled

Format
   network javascriptmode

Mode
   Privileged EXEC

no network javascriptmode

When the user accesses the switch’s web interface, the switch’s web server will deliver a HTML page that contains no JavaScript.

Format
   no network javascriptmode

Mode
   Privileged EXEC
### 3.3.4 network parms

This command sets the IP Address, subnet mask and gateway of the router. The IP Address and the gateway must be on the same subnet.

**Format**

```
network parms <ipaddr> <netmask> [gateway]
```

**Mode**

Privileged EXEC

### 3.3.5 network protocol

This command specifies the network configuration protocol to be used. If you modify this value, change is effective immediately after you saved your changes.

The parameter `bootp` indicates that the switch periodically sends requests to a Bootstrap Protocol (BootP) server or a DHCP server until a response is received.

`none` indicates that the switch should be manually configured with IP information.

Independently of the BootP and DHCP settings, HiDiscovery can be configured as an additional protocol.

**Default**

DHCP

**Format**

```
network protocol {none | bootp | dhcp | hidiscovery {off | read-only | read-write}}
```

**Mode**

Privileged EXEC
### 3.3.6 network priority

This command configures the VLAN priority or the IP DSCP value for outgoing management packets. The `<ipdscp>` is specified as either an integer from 0-63, or symbolically through one of the following keywords: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef.

**Default**

0 for both values

**Format**

```
network priority {dot1p-vlan <0-7> | ip-dscp <ipdscp> }
```

**Mode**

Privileged EXEC

---

**no network priority**

This command sets the VLAN priority or the IP DSCP value for outgoing management packets to default which means VLAN priority 0 or IP DSCP value 0 (Best effort).

**Format**

```
no network priority {dot1p-vlan | ip-dscp }
```

**Mode**

Privileged EXEC
3.3.7 serial timeout

This command specifies the maximum connect time (in minutes) without console activity. A value of 0 indicates that a console can be connected indefinitely. The time range is 0 to 160.

Default
5

Format
serial timeout <0-160>

Mode
Line Config

no serial timeout
This command sets the maximum connect time without console activity (in minutes) back to the default value.

Format
no serial timeout

Mode
Line Config
3.3.8 set prompt

This command changes the name of the prompt. The length of name may be up to 64 alphanumeric characters.

Format

    set prompt <prompt string>

Mode

    Privileged EXEC

3.3.9 show network

This command displays configuration settings associated with the switch’s network interface. The network interface is the logical interface used for in-band connectivity with the switch via any of the switch's front panel ports. The configuration parameters associated with the switch's network interface do not affect the configuration of the front panel ports through which traffic is switched or routed.

Format

    show network

Mode

    Privileged EXEC and User EXEC

System IP Address

The IP address of the interface. The factory default value is 0.0.0.0

Subnet Mask

The IP subnet mask for this interface. The factory default value is 0.0.0.0

Default Gateway

The default gateway for this IP interface. The factory default value is 0.0.0.0

Burned In MAC Address

The burned in MAC address used for in-band connectivity.
Network Configuration Protocol (BootP/DHCP)
Indicates which network protocol is being used. The options are
text:

boottp | dhcp | none.

DHCP Client ID (same as SNMP System Name)
Displays the DHCP Client ID.

Network Configuration Protocol HiDiscovery
Indicates in which way the HiDiscovery protocol is being used. The
options are off | read-only | read-write.

Management VLAN Priority
Specifies the management VLAN Priority.

Management VLAN IP-DSCP Value
Specifies the management VLAN IP-DSCP value.

Java Script Mode
Specifies if the Switch will use Java Script to start the Management
Applet. The factory default is enabled.
3.3.10 show serial

This command displays serial communication settings for the switch.

Format

    show serial

Mode

    Privileged EXEC and User EXEC

Serial Port Login Timeout (minutes)

    Specifies the time, in minutes, of inactivity on a Serial port connection, after which the Switch will close the connection. Any numeric value between 0 and 160 is allowed, the factory default is 5. A value of 0 disables the timeout.

3.3.11 show snmp-access

This command displays SNMP access information related to global and SNMP version settings. SNMPv3 is always enabled.

Format

    show snmp-access

Mode

    Privileged EXEC
### 3.3.12 show snmpcommunity

This command displays SNMP community information. Six communities are supported. You can add, change, or delete communities. The switch does not have to be reset for changes to take effect.

The SNMP agent of the switch complies with SNMP Version 1 (for more about the SNMP specification, see the SNMP RFCs). The SNMP agent sends traps through TCP/IP to an external SNMP manager based on the SNMP configuration (the trap receiver and other SNMP community parameters).

#### Format

```
show snmpcommunity
```

#### Mode

Privileged EXEC

#### SNMP Community Name

The community string to which this entry grants access. A valid entry is a case-sensitive alphanumeric string of up to 32 characters. Each row of this table must contain a unique community name.

#### Client IP Address -

An IP address (or portion thereof) from which this device will accept SNMP packets with the associated community. The requesting entity's IP address is ANDed with the Subnet Mask before being compared to the IP Address. Note: that if the Subnet Mask is set to 0.0.0.0, an IP Address of 0.0.0.0 matches all IP addresses. The default value is 0.0.0.0

#### Client IP Mask -

A mask to be ANDed with the requesting entity's IP address before comparison with IP Address. If the result matches with IP Address then the address is an authenticated IP address. For example, if the IP Address = 9.47.128.0 and the corresponding Subnet Mask = 255.255.255.0 a range of incoming IP addresses would match, i.e. the incoming IP Address could equal 9.47.128.0 - 9.47.128.255. The default value is 0.0.0.0

#### Access Mode

The access level for this community string.

#### Status

The status of this community access entry.
3.3.13 show snmptrap

This command displays SNMP trap receivers. Trap messages are sent across a network to an SNMP Network Manager. These messages alert the manager to events occurring within the switch or on the network. Six trap receivers are simultaneously supported.

Format

    show snmptrap

Mode

    Privileged EXEC

SNMP Trap Name

    The community string of the SNMP trap packet sent to the trap manager. This may be up to 32 alphanumeric characters. This string is case sensitive.

IP Address

    The IP address to receive SNMP traps from this device. Enter four numbers between 0 and 255 separated by periods.

Status

    A pull down menu that indicates the receiver's status (enabled or disabled) and allows the administrator/user to perform actions on this user entry:

    Enable - send traps to the receiver
    Disable - do not send traps to the receiver.
    Delete - remove the table entry.
3.3.14 show trapflags

This command displays trap conditions. Configure which traps the switch should generate by enabling or disabling the trap condition. If a trap condition is enabled and the condition is detected, the switch's SNMP agent sends the trap to all enabled trap receivers. The switch does not have to be reset to implement the changes. Cold and warm start traps are always generated and cannot be disabled.

**Format**

```
show trapflags
```

**Mode**

Privileged EXEC and User EXEC

**Authentication Flag**

May be enabled or disabled. The factory default is enabled. Indicates whether authentication failure traps will be sent.

**Chassis**

Indicates whether traps that are related to the chassis functionality of the switch will be sent. These functions include the signal contacts, the ACA, temperature limits exceeded, status of power supply has changed and the LLDP and SNTP features. May be enabled or disabled.

Default: enabled.

**Layer 2 Redundancy**

Indicates whether traps that are related to the layer 2 redundancy features of the switch will be sent. The HiPER-Ring and the Redundant Coupling will tell you with these traps when the main line has become inoperative or returned. May be enabled or disabled.

Default: enabled.

**Link Up/Down Flag**

May be enabled or disabled. The factory default is enabled. Indicates whether link status traps will be sent.
3.3.15 snmp-access global

This command configures the global SNMP access setting (for all SNMP versions).

**Format**

```
snmp-access global {disable|enable|read-only}
```

**Mode**

Global Config

**disable**

Disable SNMP access to this switch, regardless of the SNMP version used.

**enable**

Enable SNMP read and write access to this switch, regardless of the SNMP version used.

**read-only**

Enable SNMP read-only access to this switch (disable write access), regardless of the SNMP version used.
3.3.16 \texttt{snmp-access version}

This command configures the SNMP version specific access mode for SNMPv1 and SNMPv2.

\textbf{Format}

\begin{verbatim}
    snmp-access version \{all|v1|v2\} \{disable|enable\}
\end{verbatim}

\textbf{Mode}

\begin{verbatim}
    Global Config
\end{verbatim}

- all
  Enable or disable SNMP access by all protocol versions (v1 and v2).

- v1
  Enable or disable SNMP access by v1.

- v2
  Enable or disable SNMP access by v2.

\textbf{Note:} The SNMPv3 is always allowed and can only be disabled or restricted by the global command (\texttt{snmp-access global ...}).
3.3.17 snmp-server

This command sets the name and the physical location of the switch, and the organization responsible for the network. The range for name, location and contact is from 0 to 64 alphanumeric characters.

Default
None

Format
snmp-server

{community <name> |
ipaddr <ipaddr> <name> |
ipmask <ipmask> <name> |
mode <name> |
ro <name> |
rw <name> |
contact <con> |
enable traps { chassis | l2redundancy |
linkmode | stpmode }
location <loc> |
sysname <name> }

Mode
Global Config
### 3.3.18 snmp-server community

This command adds a new SNMP community name. A community name is a name associated with the switch and with a set of SNMP managers that manage it with a specified privileged level. The length of name can be up to 32 case-sensitive characters.

**Note:** Community names in the SNMP community table must be unique. When making multiple entries using the same community name, the first entry is kept and processed and all duplicate entries are ignored.

**Default**

Two default community names: Public and Private. You can replace these default community names with unique identifiers for each community. The default values for the remaining four community names are blank.

**Format**

```
snmp-server community <name>
```

**Mode**

Global Config

---

**no snmp-server community**

This command removes this community name from the table. The name is the community name to be deleted.

**Format**

```
no snmp-server community <name>
```

**Mode**

Global Config
### 3.3.19 snmp-server community ipaddr

This command sets a client IP address for an SNMP community. The address is the associated community SNMP packet sending address and is used along with the client IP mask value to denote a range of IP addresses from which SNMP clients may use that community to access the device. A value of 0.0.0.0 allows access from any IP address. Otherwise, this value is ANDed with the mask to determine the range of allowed client IP addresses. The name is the applicable community name.

**Default**

0.0.0.0

**Format**

```
snmp-server community ipaddr <ipaddr> <name>
```

**Mode**

Global Config

---

### no snmp-server community ipaddr

This command sets a client IP address for an SNMP community to 0.0.0.0. The name is the applicable community name.

**Format**

```
no snmp-server community ipaddr <name>
```

**Mode**

Global Config
### 3.3.20 snmp-server community ipmask

This command sets a client IP mask for an SNMP community. The address is the associated community SNMP packet sending address and is used along with the client IP address value to denote a range of IP addresses from which SNMP clients may use that community to access the device. A value of 255.255.255.255 will allow access from only one station, and will use that machine's IP address for the client IP Address. A value of 0.0.0.0 will allow access from any IP address. The name is the applicable community name.

**Default**

```
0.0.0.0
```

**Format**

```
snmp-server community ipmask <ipmask> <name>
```

**Mode**

```
Global Config
```

---

**no** **snmp-server community ipmask**

This command sets a client IP mask for an SNMP community to 0.0.0.0. The name is the applicable community name. The community name may be up to 32 alphanumeric characters.

**Format**

```
no snmp-server community ipmask <name>
```

**Mode**

```
Global Config
```
### 3.3.21 snmp-server community mode

This command activates an SNMP community. If a community is enabled, an SNMP manager associated with this community manages the switch according to its access right. If the community is disabled, no SNMP requests using this community are accepted. In this case the SNMP manager associated with this community cannot manage the switch until the Status is changed back to Enable.

**Default**

The default private and public communities are enabled by default. The four undefined communities are disabled by default.

**Format**

```
snmp-server community mode <name>
```

**Mode**

Global Config

---

**no snmp-server community mode**

This command deactivates an SNMP community. If the community is disabled, no SNMP requests using this community are accepted. In this case the SNMP manager associated with this community cannot manage the switch until the Status is changed back to Enable.

**Format**

```
no snmp-server community mode <name>
```

**Mode**

Global Config
3.3.22 snmp-server community ro

This command restricts access to switch information. The access mode is read-only (also called public).

Format
   snmp-server community ro <name>

Mode
   Global Config

3.3.23 snmp-server community rw

This command restricts access to switch information. The access mode is read/write (also called private).

Format
   snmp-server community rw <name>

Mode
   Global Config

3.3.24 snmp-server location

This command configures the system location.

Format
   snmp-server location <system location>

Mode
   Global Config
3.3.25 snmp-server sysname

This command configures the system name.

Format

```
snmp-server sysname <system name>
```

Mode

Global Config

3.3.26 snmp-server enable traps

This command enables the Authentication Trap Flag.

Default

enabled

Format

```
snmp-server enable traps
```

Mode

Global Config

no snmp-server enable traps

This command disables the Authentication Trap Flag.

Format

```
no snmp-server enable traps
```

Mode

Global Config
3.3.27 `snmp-server enable traps chassis`

Configures whether traps that are related to the chassis functionality of the switch will be sent. These functions include the signal contacts, the ACA, temperature limits exceeded, status of power supply has changed and the LLDP and SNTP features. May be enabled or disabled. Default: enabled.

**Default**

enabled

**Format**

`snmp-server enable traps chassis`

**Mode**

Global Config

---

**no snmp-server enable traps chassis**

This command disables chassis traps for the entire switch.

**Format**

`no snmp-server enable traps chassis`

**Mode**

Global Config
3.3.28 `snmp-server enable traps l2redundancy`

Indicates whether traps that are related to the layer 2 redundancy features of the switch will be sent. The HiPER-Ring and the Redundant Coupling will tell you with these traps when the main line has become inoperative or returned. May be enabled or disabled. Default: enabled.

**Default**

enabled

**Format**

`snmp-server enable traps l2redundancy`

**Mode**

Global Config

---

**no snmp-server enable traps l2redundancy**

This command disables layer 2 redundancy traps for the entire switch.

**Format**

`no snmp-server enable traps l2redundancy`

**Mode**

Global Config
3.3.29 snmp-server enable traps linkmode

This command enables Link Up/Down traps for the entire switch. When enabled, link traps are sent only if the Link Trap flag setting associated with the port is enabled (see 'snmp trap link-status' command).

Default
   enabled

Format
   snmp-server enable traps linkmode

Mode
   Global Config

no snmp-server enable traps linkmode

This command disables Link Up/Down traps for the entire switch.

Format
   no snmp-server enable traps linkmode

Mode
   Global Config
3.3.30 `snmp-server enable traps stpmode`

This command enables the sending of new root traps and topology change notification traps.

**Default**

`enabled`

**Format**

```
snmp-server enable traps stpmode
```  

**Mode**

`Global Config`

---

**no snmp-server enable traps stpmode**

This command disables the sending of new root traps and topology change notification traps.

**Format**

```
no snmp-server enable traps stpmode
```  

**Mode**

`Global Config`
3.3.31 snmptrap

This command adds an SNMP trap name. The maximum length of name is 32 case-sensitive alphanumeric characters.

Default
The default name for the six undefined community names is Delete.

Format
snmptrap <name> <ipaddr> [snmpversion snmpv1]

Mode
Global Config

no snmptrap
This command deletes trap receivers for a community.

Format
no snmptrap <name> <ipaddr>

Mode
Global Config
3.3.32 snmptrap ipaddr

This command assigns an IP address to a specified community name. The maximum length of name is 32 case-sensitive alphanumeric characters.

**Note:** IP addresses in the SNMP trap receiver table must be unique. If you make multiple entries using the same IP address, the first entry is retained and processed. All duplicate entries are ignored.

**Format**

```
snmptrap ipaddr <name> <ipaddr> <ipaddrnew>
```

**Mode**

Global Config

**ipaddr**

Enter the old IP Address.

**ipaddrnew**

Enter the new IP Address.
### 3.3.33 snmptrap mode

This command activates or deactivates an SNMP trap. Enabled trap receivers are active (able to receive traps). Disabled trap receivers are inactive (not able to receive traps).

**Format**

```
snmptrap mode <name> <ipaddr>
```

**Mode**

Global Config

---

**no snmptrap mode**

This command deactivates an SNMP trap. Disabled trap receivers are inactive (not able to receive traps).

**Format**

```
no snmptrap mode <name> <ipaddr>
```

**Mode**

Global Config
3.3.34 snmptrap snmpversion

This command configures SNMP trap version for a specified community.

Format

    snmptrap snmpversion <name> <ipAddr>
    {snmpv1 | snmpv2}

Mode

    Global Config

name

    Enter the community name.

ipAddr

    Enter the IP Address.

snmpv1

    Use SNMP v1 to send traps.

snmpv2

    Use SNMP v2 to send traps.
3.4 Syslog Commands

This section provides a detailed explanation of the Syslog commands. The commands are divided into two functional groups:

- Show commands display spanning tree settings, statistics, and other information.
- Configuration Commands configure features and options of the device. For every configuration command there is a show command that displays the configuration setting.

3.4.1 logging buffered

This command enables logging to an in-memory log where up to 128 logs are kept.

Default

enabled

Format

logging buffered

Mode

Global Config

no logging buffered

This command disables logging to in-memory log.

Format

no logging buffered
3.4.2 logging buffered wrap

This command enables wrapping of in-memory logging when full capacity reached. Otherwise when full capacity is reached, logging stops.

Default

wrap

Format

logging buffered wrap

Mode

Privileged EXEC

no logging buffered wrap

This command disables wrapping of in-memory logging and configures logging to stop when capacity is full.

Format

no logging buffered wrap
3.4.3 logging cli-command

This command enables the CLI command Logging feature. The Command Logging component enables the switch software to log all Command Line Interface (CLI) commands issued on the system.

Default

disabled

Format

logging cli-command

Mode

Global Config

no logging cli-command

This command disables the CLI command Logging feature.

Format

no logging cli-command
3.4.4 logging console

This command enables logging to the console. The `<severitylevel>` value is specified as either an integer from 0 to 7 or symbolically through one of the following keywords: emergency (0), alert (1), critical (2), error (3), warning (4), notice (5), informational (6), debug (7).

Default

disabled; alert

Format

logging console [severitylevel] | <[0-7]>

Mode

Global Config

severitylevel | [0-7]

Enter Logging Severity Level (emergency|0, alert|1, critical|2, error|3, warning|4, notice|5, info|6, debug|7).

Note: selecting a lower severity level (larger number) will include all messages from higher severity levels (smaller numbers).

no logging console

This command disables logging to the console.

Format

no logging console
3.5 Device Configuration Commands

3.5.1 auto-negotiate

This command enables automatic negotiation on a port. The default value is enable.

Format
   auto-negotiate

Mode
   Interface Config

no auto-negotiate

This command disables automatic negotiation on a port.

Format
   no auto-negotiate

Mode
   Interface Config
3.5.2 cable-crossing

Enable or disable the cable crossing function.

**Note:** The cable-crossing settings become effective for a certain port, if auto-negotiate is disabled for this port.
The cable-crossing settings are irrelevant for a certain port, if auto-negotiate is enabled for this port.

**Note:** The cable-crossing function is available for the RS20/RS30/RS40, MS20/MS30, RSR20/RSR30, MACH 1000, PowerMICE and OCTOPUS 8M/16M/24M devices.

**Format**

```
cable-crossing {enable|disable}
```

**Mode**

Interface Config

cable-crossing enable

The device swaps the port output and port input of the TP port.

cable-crossing disable

The device does not swap the port output and port input of the TP port.
3.5.3 auto-negotiate all

This command enables automatic negotiation on all ports. The default value is enable.

**Format**

auto-negotiate all

**Mode**

Global Config

**no auto-negotiate all**

This command disables automatic negotiation on all ports.

**Format**

no auto-negotiate all

**Mode**

Global Config
3.5.4  macfilter

This command adds a static MAC filter entry for the MAC address <macaddr> on the VLAN <vlanid>. The <macaddr> parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6.

The restricted MAC Addresses are: 00:00:00:00:00:00, 01:80:C2:00:00:00 to 01:80:C2:00:00:0F, 01:80:C2:00:00:20 to 01:80:C2:00:00:21, and FF:FF:FF:FF:FF:FF.

The <vlanid> parameter must identify a valid VLAN (1 to 4042).

Up to 100 static MAC filters may be created.

**Format**

```
macfilter <macaddr> <vlanid>
```

**Mode**

- Global Config

---

**no macfilter**

This command removes all filtering restrictions and the static MAC filter entry for the MAC address <macaddr> on the VLAN <vlanid>. The <macaddr> parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6.

The <vlanid> parameter must identify a valid VLAN (1 to 4042).

**Format**

```
no macfilter <macaddr> <vlanid>
```

**Mode**

- Global Config
3.5.5 macfilter adddest

This command adds the interface to the destination filter set for the MAC filter with the given \texttt{<macaddr>} and VLAN of \texttt{<vlanid>}. The \texttt{<macaddr>} parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The \texttt{<vlanid>} parameter must identify a valid VLAN (1-4042).

**Format**

```
macfilter adddest <macaddr> <vlanid>
```

**Mode**

Interface Config

---

**no macfilter adddest**

This command removes a port from the destination filter set for the MAC filter with the given \texttt{<macaddr>} and VLAN of \texttt{<vlanid>}. The \texttt{<macaddr>} parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6.

The \texttt{<vlanid>} parameter must identify a valid VLAN (1-4042).

**Format**

```
no macfilter adddest <macaddr> <vlanid>
```

**Mode**

Interface Config
3.5.6  macfilter adddest all

This command adds all interfaces to the destination filter set for the MAC filter with the given <macaddr> and VLAN of <vlanid>. The <macaddr> parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6.

The <vlanid> parameter must identify a valid VLAN (1 to 4042).

Format

macfilter adddest {all | <macaddr> <vlanid>}

Mode

Global Config

no macfilter adddest all

This command removes all ports from the destination filter set for the MAC filter with the given <macaddr> and VLAN of <vlanid>. The <macaddr> parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6.

The <vlanid> parameter must identify a valid VLAN (1 to 4042).

Format

no macfilter adddest [all | <macaddr> <vlanid>]

Mode

Global Config
3.5.7 monitor session <session-id>

This command configures a probe port and a monitored port for monitor session (port monitoring). The first slot/port is the source monitored port and the second slot/port is the destination probe port. If this command is executed while port monitoring is enabled, it will have the effect of changing the probe and monitored port values.

Format

```
monitor session <session-id>
  [mode | {source | destination}
    interface <slot/port>]
```

Mode

- Global Config

destination
- Configure the probe interface.

tmode
- Enable/Disable port mirroring session.
  Note: does not affect the source or destination interfaces.

source
- Configure the source interface.

session-id
- Session number (currently, session number 1 is supported).

no monitor session<session-id>

This command removes the monitor session (port monitoring) designation from both the source probe port and the destination monitored port.

Format

```
no monitor session <session-id> [mode]
```

Mode

- Global Config

session-id
- Session number (currently, session number 1 is supported).
### 3.5.8 monitor session <session-id>mode

This command configures the monitor session (port monitoring) mode to enable. The probe and monitored ports must be configured before monitor session (port monitoring) can be enabled. If enabled, the probe port will monitor all traffic received and transmitted on the physical monitored port. It is not necessary to disable port monitoring before modifying the probe and monitored ports.

**Default**

disabled

**Format**

```shell
monitor session <session-id>mode
```

**Mode**

Global Config

**session-id**

Session number (currently, session number 1 is supported).

---

**no monitor session <session-id>mode**

This command sets the monitor session (port monitoring) mode to disable.

**Format**

```shell
no monitor session <session-id>mode
```

**Mode**

Global Config

**session-id**

Session number (currently, session number 1 is supported).
3.5.9  monitor session <session-id> source/destination

This command allows you to configure and activate the port mirroring function of the switch. Port mirroring is when the data traffic of a source port is copied to a specified destination port. The data traffic at the source port is not influenced by port mirroring. A management tool connected at the specified port, e.g., an RMON probe, can thus monitor the data traffic of the source port.

**Note:** In active port mirroring, the specified destination port is used solely for observation purposes.

**Default**

none

**Format**

```
monitor session {source | destination} interface <slot/port>
```

**Mode**

Global Config

**session-id**

Session number (currently, session number 1 is supported).

**no monitor session <session-id> source/destination**

This command resets the monitor session (port monitoring) source/destination. The port will be removed from port mirroring

**Format**

```
no monitor session <session-id> {source | destination} interface
```

**Mode**

Global Config

**session-id**

Session number (currently, session number 1 is supported).
3.5.10 set igmp (Global Config Mode)

This command enables IGMP Snooping on the system. The default value is disable.

**Note:** The IGMP snooping application supports the following:
- Global configuration or per interface configuration.
- Validation of the IP header checksum (as well as the IGMP header checksum) and discarding of the frame upon checksum error.
- Maintenance of the forwarding table entries based on the MAC address versus the IP address.
- Flooding of unregistered multicast data packets to all ports.

**Format**

```
set igmp
```

**Mode**

Global Config

**no set igmp**

This command disables IGMP Snooping on the system.

**Format**

```
no set igmp
```

**Mode**

Global Config
3.5.11 set igmp (Interface Config Mode)

This command enables IGMP Snooping on a selected interface.

Default
   enabled

Format
   set igmp

Mode
   Interface Config

no set igmp

This command disables IGMP Snooping on a selected interface.

Format
   no set igmp

Mode
   Interface Config
3.5.12 set igmp aging-time-unknown

This command configures the IGMP Snooping aging time for unknown multicast frames (unit: seconds, min.: 3, max.: 3,600, default: 260).

Format

set igmp aging-time-unknown <3-3600>

Mode

Global Config

3.5.13 set igmp automatic-mode

If enabled, this port is allowed to be set as static query port automatically, if the LLDP protocol has found a switch or router connected to this port. Use the command's normal form to enable the feature, the 'no' form to disable it.

Default

disabled (RS20: enabled)

Format

set igmp automatic-mode

Mode

Interface Config
3.5.14 set igmp forward-all

This command activates the forwarding of multicast frames to this interface even if the given interface has not received any reports by hosts. N. B.: this applies only to frames that have been learned via IGMP Snooping. The purpose is that an interface (e. g. a HIPER Ring's ring port) may need to forward all such frames even if no reports have been received on it. This enables faster recovery from ring interruptions for multicast frames.

Default
disabled

Format
set igmp forward-all

Mode
Interface Config

no set igmp forward-all

This command disables the forwarding of all multicast frames learned via IGMP Snooping on a selected interface.

Format
no set igmp forward-all

Mode
Interface Config
3.5.15 set igmp forward-unknown

This command defines how to handle unknown multicast frames. This command is available for MS20/MS30.

Format

```
set igmp forward-unknown
    { discard | flood | query-ports }
```

Mode

- **Global Config**

**discard**

Unknown multicast frames will be discarded.

**flood**

Unknown multicast frames will be flooded.

**query-ports**

Unknown multicast frames will be forwarded only to query ports.
### 3.5.16 set igmp static-query-port

This command activates the forwarding of IGMP membership report frames to this interface even if the given interface has not received any queries. The purpose is that a port may need to forward such frames even if no queries have been received on it (e.g., if a router is connected to the interface that sends no queries).

**Default**

disabled

**Format**

```
set igmp static-query-port
```

**Mode**

Interface Config

---

**no set igmp**

This command disables the unconditional forwarding of IGMP membership report frames to this interface.

**Format**

```
no set igmp static-query-port
```

**Mode**

Interface Config
3.5.17 set igmp groupmembershipinterval

This command sets the IGMP Group Membership Interval time on the system. The Group Membership Interval time is the amount of time in seconds that a switch will wait for a report from a particular group on a particular interface before deleting the interface from the entry. This value must be greater than the IGMP Maximum Response time value. The range is 3 to 3,600 seconds.

Default

260

Format

set igmp groupmembershipinterval <3-3600>

Mode

Global Config

no set igmp groupmembershipinterval

This command sets the IGMP Group Membership Interval time on the system to 260 seconds.

Format

no set igmp groupmembershipinterval

Mode

Global Config
3.5.18 set igmp interfacemode

This command enables IGMP Snooping on all interfaces. If an interface which has IGMP Snooping enabled is enabled for port-based routing or is enlisted as a member of a link-aggregation (LAG), IGMP Snooping functionality will be disabled on that interface. IGMP Snooping functionality will subsequently be re-enabled if routing is disabled or link-aggregation (LAG) membership is removed from an interface that has IGMP Snooping enabled.

**Format**

```
set igmp interfacemode
```

**Mode**

Global Config

---

**no set igmp interfacemode**

This command disables IGMP Snooping on all interfaces.

**Format**

```
no set igmp interfacemode
```

**Mode**

Global Config
3.5.19 set igmp lookup-interval-unknown

This command configures the IGMP Snooping lookup response time for unknown multicast frames (unit: seconds, min.: 2, max.: 3,599, default: 125).

**Format**

```
set igmp lookup-interval-unknown <2-3599>
```

**Mode**

- Global Config

**<2-3599>**

Enter the IGMP Snooping lookup response time for unknown multicast frames (unit: seconds, min.: 2, max.: 3,599, default: 125).

---

3.5.20 set igmp lookup-resp-time-unknown

This command configures the IGMP Snooping lookup interval for unknown multicast frames (unit: seconds, min.: 1, max.: 3,598, default: 10).

**Format**

```
set igmp lookup-resp-time-unknown <1-3598>
```

**Mode**

- Global Config

**<1-3598>**

Enter the IGMP Snooping lookup interval for unknown multicast frames (unit: seconds, min.: 1, max.: 3,598, default: 10).
3.5.21 set igmp maxresponse

This command sets the IGMP Maximum Response time on the system. The Maximum Response time is the amount of time in seconds that a switch will wait after sending a query in response to a received leave message, before deleting the multicast group received in the leave message. If the switch receives a report in response to the query within the maxresponse time, then the multicast group is not deleted. This value must be less than the IGMP Query Interval time value. The range is 1 to 3,598 seconds.

Default
10

Format
set igmp maxresponse <1-3598>

Mode
Global Config

Note: the IGMP Querier's max. response time was also set. It is always the same value as the IGMP Snooping max. response time.

no set igmp maxresponse

This command sets the IGMP Maximum Response time on the system to 10 seconds.

Format
no set igmp maxresponse

Mode
Global Config
### 3.5.22 set igmp querier max-response-time

Configure the IGMP Snooping Querier's maximum response time. The range is 1 to 3,598 seconds. The default value is 10 seconds.

**Default**

10

**Format**

```
set igmp querier max-response-time <1-3598>
```

**Mode**

Global Config

**Note:** The IGMP Snooping max. response time was also set. It is always the same value as the IGMP Querier’s max. response time.

### 3.5.23 set igmp querier protocol-version

Configure the IGMP Snooping Querier's protocol version (1, 2 or 3).

**Default**

2

**Format**

```
set igmp querier protocol-version {1 | 2 | 3}
```

**Mode**

Global Config
3.5.24 set igmp querier status

Configure the IGMP Snooping Querier's administrative status (enable or disable).

Default
disable

Format
set igmp querier status {enable | disable}

Mode
Global Config

3.5.25 set igmp querier tx-interval

Configure the IGMP Snooping Querier's transmit interval. The range is 2 to 3,599 seconds.

Default
125

Format
set igmp querier tx-interval <2-3599>

Mode
Global Config
3.5.26 set igmp query-ports-to-filter

This command enables or disables the addition of query ports to multicast filter portmasks. The setting can be enable or disable.

Default
   Disable

Format
   set igmp query-ports-to-filter {enable | disable}

Mode
   Global Config

enable
   Addition of query ports to multicast filter portmasks.

disable
   No addition of query ports to multicast filter portmasks.
3.5.27 selftest ramtest

Enable or disable the RAM test for a cold start of the device. Deactivating the RAM test cuts the booting time for a cold start of the device. Default: enabled.

Format

```
selftest ramtest {disable|enable}
```

Mode

```
Global Config
```

- `selftest ramtest disable`
  - Disable the ramtest.

- `selftest ramtest enable`
  - Enable the ramtest. This is the default.

3.5.28 selftest reboot-on-error

Enable or disable a restart due to an undefined software or hardware state. Default: disabled.

Format

```
selftest reboot-on-error {disable|enable}
```

Mode

```
Global Config
```

- `selftest reboot-on-error disable`
  - Disable the reboot-on-error function. This is the default.

- `selftest reboot-on-error enable`
  - Enable the reboot-on-error function.
### 3.5.29 show igmpsnooping

This command displays IGMP Snooping information. Configured information is displayed whether or not IGMP Snooping is enabled. Status information is only displayed when IGMP Snooping is enabled.

**Format**

```
show igmpsnooping
```

**Mode**

*Privileged EXEC and User EXEC*

**Admin Mode**

This indicates whether or not IGMP Snooping is globally enabled on the switch.

**Forwarding of Unknown Frames**

This displays if and how unknown multicasts are forwarded. The setting can be Discard, Flood or Query Ports. The default is Query Ports.

**Group Membership Interval**

This displays the IGMP Group Membership Interval. This is the amount of time a switch will wait for a report for a particular group on a particular interface before it sends a query on that interface. This value may be configured.

**Multicast Control Frame Count**

This displays the number of multicast control frames that are processed by the CPU.

**Interfaces Enabled for IGMP Snooping**

This is the list of interfaces on which IGMP Snooping is enabled. Additionally, if a port has a special function, it will be shown to the right of its slot/port number. There are 3 special functions: Forward All, Static Query Port and Learned Query Port.

**Querier Status (the administrative state).**

This displays the IGMP Snooping Querier's administrative status.

**Querier Mode (the actual state, read only)**

This displays the IGMP Snooping Querier's operating status.
3.5 Device Configuration Commands

Querier Transmit Interval
   This displays the IGMP Snooping Querier's transmit interval in seconds.

Querier Max. Response Time
   This displays the IGMP Snooping Querier's maximum response time in seconds.

Querier Protocol Version
   This displays the IGMP Snooping Querier's protocol version number.
3.5.30 show mac-filter-table igmpsnooping

This command displays the IGMP Snooping entries in the Multicast Forwarding Database (MFDB) table.

**Format**

```
show mac-filter-table igmpsnooping
```

**Mode**

Privileged EXEC and User EXEC

**Mac Address**

A multicast MAC address for which the switch has forwarding and or filtering information. The format is two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB.

**Type**

This displays the type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.

**Description**

The text description of this multicast table entry.

**Interfaces**

The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).
3.5.31 show mac-filter-table multicast

This command displays the Multicast Forwarding Database (MFDB) information. If the command is entered with no parameter, the entire table is displayed. This is the same as entering the optional all parameter. The user can display the table entry for one MAC Address by specifying the MAC address as an optional parameter.

**Format**

```
show mac-filter-table multicast
[<macaddr> <1-4042>]
```

**Mode**

Privileged EXEC and User EXEC

**Mac Address**

A multicast MAC address for which the switch has forwarding and or filtering information. The format is two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB.

**Type**

This displays the type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.

**Component**

The component that is responsible for this entry in the Multicast Forwarding Database. Possible values are IGMP Snooping and Static Filtering.

**Description**

The text description of this multicast table entry.

**Interfaces**

The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

**Forwarding Interfaces**

The resultant forwarding list is derived from combining all the component’s forwarding interfaces and removing the interfaces that are listed as the static filtering interfaces.
3.5.32 show mac-filter-table static

This command displays the Static MAC Filtering information for all Static MAC Filters. If all is selected, all the Static MAC Filters in the system are displayed. If a macaddr is entered, a vlan must also be entered and the Static MAC Filter information will be displayed only for that MAC address and VLAN.

Format

show mac-filter-table static {<macaddr> <vlanid> | all}

Mode

Privileged EXEC and User EXEC

MAC Address

Is the MAC Address of the static MAC filter entry.

VLAN ID

Is the VLAN ID of the static MAC filter entry.

Source Port(s)

Indicates the source port filter set's slot and port(s).

Destination Port(s)

Indicates the destination port filter set's slot and port(s).
### 3.5.33 show mac-filter-table staticfiltering

This command displays the Static Filtering entries in the Multicast Forwarding Database (MFDB) table.

**Format**

```
show mac-filter-table staticfiltering
```

**Mode**

Privileged EXEC and User EXEC

**Mac Address**

A unicast MAC address for which the switch has forwarding and or filtering information. The format is 6 or 8 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB.

**Type**

This displays the type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.

**Description**

The text description of this multicast table entry.

**Interfaces**

The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).
3.5.34 show mac-filter-table stats

This command displays the Multicast Forwarding Database (MFDB) statistics.

**Format**

```
show mac-filter-table stats
```

**Mode**

Privileged EXEC and User EXEC

**Total Entries**

This displays the total number of entries that can possibly be in the Multicast Forwarding Database table.

**Most MFDB Entries Ever Used**

This displays the largest number of entries that have been present in the Multicast Forwarding Database table. This value is also known as the MFDB high-water mark.

**Current Entries**

This displays the current number of entries in the Multicast Forwarding Database table.
3.5.35 show monitor session

This command displays the Port monitoring information for the system.

Format

    show monitor session <Session Number>

Mode

    Privileged EXEC and User EXEC

Session

    Display port monitor session settings.

Session Number

    Session Number. Enter 1 for the Session Number.

Port Monitor Mode

    indicates whether the Port Monitoring feature is enabled or disabled. The possible values are enable and disable.

Probe Port slot/port

    is the slot/port configured as the probe port. If this value has not been configured, 'Not Configured' will be displayed.

Monitored Port slot/port

    is the slot/port configured as the monitored port. If this value has not been configured, 'Not Configured' will be displayed.
3.5.36 show port

This command displays port information.

Format

    show port {<slot/port> | all} [name]

Mode

    Privileged EXEC and User EXEC

Slot/Port

    Valid slot and port number separated by forward slashes.

Name

    When the optional command parameter name was specified, the output is different. It specifically includes the Interface Name as the second column, followed by other basic settings that are also shown by the normal command without the command parameter name.

Type

    If not blank, this field indicates that this port is a special type of port. The possible values are:
    Mon - this port is a monitoring port. Look at the Port Monitoring screens to find out more information.
    LA Mbr - this port is a member of a Link Aggregation (LAG).
    Probe - this port is a probe port.

Admin Mode

    Indicates the Port control administration state. The port must be enabled in order for it to be allowed into the network. - May be enabled or disabled. The factory default is enabled.

Physical Mode

    Indicates the desired port speed and duplex mode. If auto-negotiation support is selected, then the duplex mode and speed will be set from the auto-negotiation process. Note that the port's maximum capability (full duplex -100M) will be advertised. Otherwise, this object will determine the port's duplex mode and transmission rate. The factory default is Auto.

Physical Status

    Indicates the port speed and duplex mode.

Link Status

    Indicates whether the Link is up or down.
3.5.37 show selftest

This command displays switch configuration information.

**Format**

```
show selftest
```

**Mode**

Privileged EXEC and User EXEC

**Ramtest state**

May be enabled or disabled. The factory default is enabled.

**Reboot on error**

May be enabled or disabled. The factory default is enabled.
3.5.38  **shutdown**

This command disables a port.

**Default**

enabled

**Format**

shutdown

**Mode**

Interface Config

■ **no shutdown**

This command enables a port.

**Format**

no shutdown

**Mode**

Interface Config
3.5.39 **shutdown all**

This command disables all ports.

**Default**

enabled

**Format**

`shutdown all`

**Mode**

Global Config

---

**no shutdown all**

This command enables all ports.

**Format**

`no shutdown all`

**Mode**

Global Config
3.5.40 `snmp trap link-status`

This command enables link status traps by interface.

**Note:** This command is valid only when the Link Up/Down Flag is enabled. See ‘snmp-server enable traps linkmode’ command.

**Format**

```
snmp trap link-status
```

**Mode**

```
Interface Config
```

---

**no snmp trap link-status**

This command disables link status traps by interface.

**Note:** This command is valid only when the Link Up/Down Flag is enabled. See ‘snmp-server enable traps linkmode’ command).

**Format**

```
no snmp trap link-status
```

**Mode**

```
Interface Config
```
3.5.41 snmp trap link-status all

This command enables link status traps for all interfaces.

Note: This command is valid only when the Link Up/Down Flag is enabled (see “snmp-server enable traps linkmode”).

Format
   snmp trap link-status all

Mode
   Global Config

no snmp trap link-status all

This command disables link status traps for all interfaces.

Note: This command is valid only when the Link Up/Down Flag is enabled (see “snmp-server enable traps linkmode”).

Format
   no snmp trap link-status all

Mode
   Global Config
3.5.42 spanning-tree bpdumigrationcheck

This command enables BPDU migration check on a given interface. This will force the specified port to transmit RST or MST BPDUs. The all option enables BPDU migration check on all interfaces.

**Format**

```
spanning-tree bpdumigrationcheck {<slot/port>|all}
```

**Mode**

Global Config

**no spanning-tree bpdumigrationcheck**

This command disables BPDU migration check on a given interface. The all option disables BPDU migration check on all interfaces.

**Format**

```
no spanning-tree bpdumigrationcheck {<slot/port>|all}
```

**Mode**

Global Config
3.5.43 speed

This command sets the speed and duplex setting for the interface.

Format

```
speed {<100 | 10> <half-duplex | full-duplex> | 1000 full-duplex}
```

Mode

Interface Config

Acceptable values are:

- **100h**
  - 100BASE-T half duplex
- **100f**
  - 100BASE-T full duplex
- **10h**
  - 10BASE-T half duplex
- **10f**
  - 10BASE-T full duplex
3.6 User Account Management Commands

These commands manage user accounts.

3.6.1 show loginssession

This command displays login session information about the CLI sessions which are currently open on the local device.

Format

```
show loginssession
```

Mode

Privileged EXEC and User EXEC

ID

Login Session ID

User Name

The name the user will use to login using the serial port.

Connection From

EIA-232 for the serial port connection.

Idle Time

Time this session has been idle.

Session Time

Total time this session has been connected.
3.6.2 show users

This command displays the configured user names and their settings. This command is only available for users with readwrite privileges. The SNMPv3 fields will only be displayed if SNMP is available on the system.

Format

    show users

Mode

    Privileged EXEC

User Name

    The name the user will use to login using the serial port or Web. A new user may be added to the switch by entering a name in a blank entry. The user name may be up to eight characters, and is not case sensitive. Two users are included as the factory default, ‘admin’ and ‘user’

Access Mode

    Shows whether the operator is able to change parameters on the switch (Read/Write) or is only able to view them (Read Only). As a factory default, the ‘admin’ user has Read/Write access and the ‘user’ has Read Only access. There can only be one Read/Write user and up to five Read Only users.

SNMPv3 Access Mode

    This field displays the SNMPv3 Access Mode. If the value is set to ReadWrite, the SNMPv3 user will be able to set and retrieve parameters on the system. If the value is set to ReadOnly, the SNMPv3 user will only be able to retrieve parameter information. The SNMPv3 access mode may be different than the CLI and Web access mode.

SNMPv3 Authentication

    This field displays the authentication protocol to be used for the specified login user.

SNMPv3 Encryption

    This field displays the encryption protocol to be used for the specified login user.
3.6.3  users defaultlogin

This command assigns the authentication login list to use for non-configured users when attempting to log in to the system. This setting is overridden by the authentication login list assigned to a specific user if the user is configured locally. If this value is not configured, users will be authenticated using local authentication only.

Format

    users defaultlogin <listname>

Mode

    Global Config

listname

    Enter an alphanumeric string of not more than 15 characters.
3.6.4 users login <user>

Enter user name.

Format

```
users login <user> <listname>
```

Mode

Global Config

Note:

When assigning a list to the 'admin' account, include an authentication method that allows administrative access even when remote authentication is unavailable (use 'authentication login <listname> [method1 [method2 [method3]]]').

no users login <user>

This command removes an operator.

Format

```
no users login <user> <listname>
```

Mode

Global Config

Note:

The ‘admin’ user account cannot be deleted.
3.6.5  users access

This command sets access for a user: readonly/readwrite.

Format

    users access <username> {readonly | readwrite}

Mode

    Global Config

<username>

Enter a name up to 32 alphanumeric characters in length.

readonly

Enter the access mode as readonly.

readwrite

Enter the access mode as readwrite.

no users access

This command deletes access for a user.

Format

    no users access <username>

Mode

    Global Config
3.6.6 users name

This command adds a new user (account) if space permits. The account 
<username> can be up to eight characters in length. The name may be com- 
prised of alphanumeric characters as well as the dash (‘-’) and underscore 
(‘_’). The <username> is not case-sensitive. Six user names can be defined.

**Format**

users name <username>

**Mode**

Global Config

---

**no users name**

This command removes an operator.

**Format**

no users name <username>

**Mode**

Global Config

**Note:**

The ‘admin’ user account cannot be deleted.
3.6.7 users passwd

This command is used to change a password. The password should not be more than eight alphanumeric characters in length. If a user is authorized for authentication or encryption is enabled, the password must be at least eight alphanumeric characters in length. The username and password are case-sensitive. When a password is changed, a prompt will ask for the former password. If none, press enter.

**Note:** Make sure, that the passwords of the users differ from each other. If two or more users try to choose the same password, the CLI will display an error message.

**Default**

No Password

**Format**

users passwd <username> {<password>}

**Mode**

Global Config

---

**no users passwd**

This command sets the password of an existing operator to blank. When a password is changed, a prompt will ask for the operator's former password. If none, press enter.

**Format**

no users passwd <username> {<password>}

**Mode**

Global Config
3.6.8 users snmpv3 accessmode

This command specifies the snmpv3 access privileges for the specified login user. The valid accessmode values are `readonly` or `readwrite`. The `<username>` is the login user name for which the specified access mode applies. The default is `readwrite` for ‘admin’ user; `readonly` for all other users.

Default

```
admin -- readwrite; other -- readonly
```

Format

```
users snmpv3 accessmode <username> <readonly | readwrite>
```

Mode

```
Global Config
```

**no users snmpv3 accessmode**

This command sets the snmpv3 access privileges for the specified login user as `readwrite` for the ‘admin’ user; `readonly` for all other users. The `<username>` is the login user name for which the specified access mode will apply.

Format

```
o users snmpv3 accessmode <username>
```

Mode

```
Global Config
```
3.6.9 users snmpv3 authentication

This command specifies the authentication protocol to be used for the specified login user. The valid authentication protocols are none, md5 or sha. If md5 or sha are specified, the user login password is also used as the snmpv3 authentication password and therefore must be at least eight characters in length. The `<username>` is the login user name associated with the authentication protocol.

Default

no authentication

Format

users snmpv3 authentication <username> <none | md5 | sha>

Mode

Global Config

no users snmpv3 authentication

This command sets the authentication protocol to be used for the specified login user to none. The `<username>` is the login user name for which the specified authentication protocol will be used.

Format

users snmpv3 authentication <username>

Mode

Global Config
3.7 System Utilities

This section describes system utilities.

3.7.1 clear eventlog

Clear the event log. The CLI will ask for confirmation. Answer y (yes) or n (no). The CLI displays the end of this operation.

**Format**

```
clear eventlog
```

**Mode**

Privileged EXEC
### 3.7.2 traceroute

This command is used to discover the routes that packets actually take when traveling to their destination through the network on a hop-by-hop basis. `<ipaddr>` should be a valid IP address.

The optional port parameter is the UDP port used as the destination of packets sent as part of the traceroute. This port should be an unused port on the destination system. `[port]` should be a valid decimal integer in the range of 0 (zero) to 65,535. The default value is 33,434.

**Format**

```
traceroute <ipaddr> [port]
```

**Mode**

Privileged EXEC

### 3.7.3 clear arp-table-switch

This command clears the agent’s ARP table (cache).

**Format**

```
clear arp-table-switch
```

**Mode**

Privileged EXEC
3.7.4 clear config

This command resets the configuration in RAM to the factory defaults without powering off the switch.

Format

    clear config

Mode

    Privileged EXEC

3.7.5 clear config factory

This command resets the whole configuration to the factory defaults. Configuration data and scripts stored in nonvolatile memory will also be deleted.

Format

    clear config factory

Mode

    Privileged EXEC

3.7.6 clear counters

This command clears the stats for a specified <slot/port> or for all the ports or for the entire switch based upon the argument.

Format

    clear counters {<slot/port> | all}

Mode

    Privileged EXEC
3.7.7 clear hiper-ring

This command clears the HIPER Ring configuration (deletes it).

Format
   clear hiper-ring

Mode
   Privileged EXEC

3.7.8 clear igmpsnooping

This command clears the tables managed by the IGMP Snooping function and will attempt to delete these entries from the Multicast Forwarding Database.

Format
   clear igmpsnooping

Mode
   Privileged EXEC
3.7.9 clear mac-addr-table

This command clears the switch's MAC address table (the forwarding database that contains the learned MAC addresses).

**Note:** this command does not affect the MAC filtering table.

**Format**

```
clear mac-addr-table
```

**Mode**

```
Privileged EXEC
```

3.7.10 clear pass

This command resets all user passwords to the factory defaults without powering off the switch. You are prompted to confirm that the password reset should proceed.

**Format**

```
clear pass
```

**Mode**

```
Privileged EXEC
```
3.7.11 clear signal-contact

This command clears the signal-contact output configuration. Switches the signal contact 1’s mode to auto and its manual setting to open. Switches the signal contact 2’s mode to manual and its manual setting to closed. Enables the monitoring of the power supplies for signal contact 1 only. Disables the sending of signal contact traps.

**Format**

```
clear signal-contact
```

**Mode**

Privileged EXEC
3.7.12 clear traplog

This command clears the trap log.

**Format**

```
clear traplog
```

**Mode**

Privileged EXEC

3.7.13 config-watchdog

If the function is enabled and the connection to the switch is interrupted for longer than the time specified in “timeout [s]”, the switch then loads the last configuration saved.

**Format**

```
cfg-watchdog {admin-state {disable|enable}| timeout <10..600>}
```

**Mode**

Global Config

**admin-state**

Enable or disable the Auto Configuration Undo feature (default: disabled).

**timeout**

Configure the Auto Configuration Undo timeout (unit: seconds).
3.7.14 copy

This command uploads and downloads to/from the switch. Remote URLs can be specified using tftp.

`copy` (without parameters) displays a brief explanation of the most important `copy` commands. A list of valid commands is provided below.
The command can be used to save the running configuration to nvram by specifying the source as `system:running-config` and the destination as `nvram:startup-config`.

**Default**
none

**Format**


**Mode**
Privileged EXEC

- **copy nvram:errorlog <url>**
  Uploads Errorlog file.

- **copy nvram:startup-config <url>**
  Uploads config file using <tftp://ip/filepath/fileName>. 
- **copy nvram:startup-config system:running-config**
  Uploads/Copies config file. The target is the currently running configuration.

- **copy nvram:traplog <url>**

- **copy system:running-config nvram:startup-config**
  Copies system config file. Save the running configuration to NVRAM.

- **copy system:running-config <url>**
  Copies system config file. Uploads system running-config via tftp using <tftp://ip/filepath/fileName>.

- **copy <url> nvram:startup-config**
  Downloads Config file by tftp using <tftp://ip/filepath/fileName>.

- **copy <url> system:image**
  Downloads code file by tftp using <tftp://ip/filepath/fileName>.

- **copy <url> system:running-config**
  Downloads Code/Config file using <tftp://ip/filepath/fileName>. The target is the currently running configuration.
3.7 System Utilities

**copy <url> system:bootcode**

Downloads bootcode file by tftp using `<tftp://ip/filepath/fileName>`.

### 3.7.15 device-status connection-error

This command configures the device status link error monitoring for this port.

**Default**

`ignore`

**Format**

`device-status connection-error {ignore|propagate}`

**Mode**

`Interface Config`

### 3.7.16 device-status monitor

This command configures the device-status.

**Format**

```
device-status monitor
   {aca-removal | all | connection-error |
      module-removal | power-supply-1 |
      power-supply-2 | power-supply-3-1 |
      power-supply-3-2 | power-supply-4-1 |
      power-supply-4-2 | temperature }
   {error|ignore}
device-status trap {disable|enable}
```
Mode

    Global Config

monitor

Determines the monitoring of the selected event or all events.
- **error** If the given event signals an error, the device state will also signal error,
- **ignore** Ignore the given event - even if it signals an error, the device state will not signal 'error' because of that.

trap

Configure if a trap is sent when the device status changes its state.
- **enable** enables sending traps,
- **disable** disables sending traps.

3.7.17 logout

This command resets the current serial connection.

**Note:** Save configuration changes before logging out.

**Format**

    logout

**Mode**

    Privileged EXEC
### 3.7.18 ping

This command checks if another computer is on the network and listens for connections. To use this command, configure the switch for network (in-band) connection. The source and target devices must have the ping utility enabled and running on top of TCP/IP. The switch can be pinged from any IP workstation with which the switch is connected, as long as there is a physical path between the switch and the workstation. The terminal interface sends, three pings to the target station.

**Format**

```
ping <ipaddr>
```

**Mode**

Privileged EXEC and User EXEC

---

### 3.7.19 signal-contact connection-error

This command configures the signal contact link error monitoring for this port.

**Format**

```
signal-contact connection-error {disable|enable}
```

**Mode**

Interface Config

**disable**

A link down event on this port will be not monitored by a signal contact (default).

**enable**

A link down event on this port will be monitored by a signal contact.
### 3.7.20 signal-contact

This command configures the signal contacts.

**Format**

```
signal-contact {1|2|all} {mode {auto|device-status|manual} |monitor {aca-removal|all|connection-error|module-removal |power-supply-1| power-supply-2 |power-supply-3-1|power-supply-3-2 |power-supply-4-1|power-supply-4-2 |temperature} {disable|enable} |state {closed|open} |trap {disable|enable}}
```

**Mode**

Global Config

**Contact No.**

Selection of the signal contact:
- 1 signal contact 1,
- 2 signal contact 2,
- all signal contact 1 and signal contact 2.

**mode**

Selection of the operational mode:
- auto function monitoring,
- device-status the device-status determines the signal contact’s status.
- manual manually setting the signal contact.

**monitor**

Enables or disables the monitoring of the selected event or all events.
- enable monitoring,
- disable no monitoring.

**state**

Set the manual setting of the signal contact:
- closed,
- open.

Only takes immediate effect in manual mode.
trap

Configures the sending of traps concerning the signal contact.
– enable enables sending traps,
– disable disables sending traps.
3.7.21 reboot

This command resets the switch (cold start), for warm start See “reload” on page 159. Reset means that all network connections are terminated and the boot code executes. The switch uses the stored configuration to initialize the switch. You are prompted to confirm that the reset should proceed. A successful reset is indicated by the LEDs on the switch.

Format
   reboot

Mode
   Privileged EXEC

3.7.22 reload

This command enables you to reset the switch (warm start), for cold start See “reboot” on page 159.

Note: First, the device is checking the software in the flash memory and then it resets. If a warm start is not possible, the device automatically executes a cold start.
Reset means that all network connections are terminated and the boot code executes. The switch uses the stored configuration to initialize the switch. You are prompted to confirm that the reset should proceed. A successful reset is indicated by the LEDs on the switch.

Format
   reload

Mode
   Privileged EXEC
3.8 LLDP - Link Layer Discovery Protocol

These commands show and configure the LLDP parameters in compliance with IEEE 802.1 AB.

3.8.1 show lldp

This command shows all LLDP settings.

Format
   show lldp

Mode
   Privileged EXEC and User EXEC

3.8.2 show lldp config

This command shows all LLDP configuration settings.

Format
   show lldp config

Mode
   Privileged EXEC and User EXEC
3.8.3  **show lldp config chassis**

This command shows all LLDP configuration settings concerning the entire device.

**Format**

```
show lldp config chassis
```

**Mode**

Privileged EXEC and User EXEC

---

3.8.4  **show lldp config chassis admin-state**

Display the LLDP/IEEE802.1AB functionality on this device. If disabled, the LLDP protocol is inactive but the LLDP MIBs can still be accessed.

**Format**

```
show lldp config chassis admin-state
```

**Mode**

Privileged EXEC and User EXEC
3.8.5  show lldp config chassis notification-interval

Display the LLDP minimum notification trap interval (unit: seconds).

**Format**

```
show lldp config chassis notification-interval
```

**Mode**

Privileged EXEC and User EXEC

3.8.6  show lldp config chassis re-init-delay

Display the LLDP configuration's chassis re-initialization delay (unit: seconds).

**Format**

```
show lldp config chassis re-init-delay
```

**Mode**

Privileged EXEC and User EXEC
3.8.7  show lldp config chassis tx-delay

Display the LLDP transmit delay (unit: seconds). It indicates the delay between successive LLDP frame transmissions.

Format
  show lldp config chassis tx-delay

Mode
  Privileged EXEC and User EXEC

3.8.8  show lldp config chassis tx-hold-mult

Display the LLDP transmit hold multiplier, a time-to-live value expressed as a multiple of the LLDP Message Tx Interval (tx-interval).

Format
  show lldp config chassis tx-hold-mult

Mode
  Privileged EXEC and User EXEC

3.8.9  show lldp config chassis tx-interval

Display the interval (unit: seconds) at which LLDP frames are transmitted on behalf of this LLDP agent.

Format
  show lldp config chassis tx-interval

Mode
  Privileged EXEC and User EXEC
3.8.10 show lldp config port

This command shows all LLDP configuration settings and states concerning one or all ports.

**Format**

```
show lldp config port <{slot/port|all}>
admin-state | fdb-mode | hm-mode |
max-neighbors | notification | tlv
```

**Mode**

Privileged EXEC and User EXEC

**admin-state**

Display the port's LLDP admin state (if LLDP/IEEE802.1AB frames will be transmitted and/or received).

**fdb-mode**

Display the port's LLDP FDB mode.

**hm-mode**

Display the port's LLDP Hirschmann mode.

**max-neighbors**

Display the port's max. no. of LLDP neighbors.

**notification**

Display the port's LLDP notification (trap) setting.

**tlv**

Display the port's LLDP TLV settings (they determine which information is included in the LLDP frames that are sent). The command is a group command and will output several lines of data.
3.8.11 show lldp config port tlv

This command shows all LLDP TLV configuration settings (if the given information is included in the sent LLDP frames or not) concerning one or all ports.

Format

    show lldp config port <{slot/port|all}> tlv

Mode

    Privileged EXEC and User EXEC

inlinepower

    Enable or disable the sending of the port's Power over Ethernet capabilities (PoE, IEEE 802.3af), available for devices supporting PoE.

link-aggregation

    Display the port's LLDP TLV inclusion of Link Aggregation.

mac-phy-config-state

    Display the port's LLDP TLV inclusion of MAC Phy. Cfg. State.

max-frame-size

    Display the port's LLDP TLV inclusion of Max. Frame Size.

mgmt-addr

    Display the port's LLDP TLV inclusion of Management Address.

port-desc

    Display the port's LLDP TLV inclusion of Port Description.

protocol

    Display the port's LLDP TLV inclusion of Protocol.

sys-cap

    Display the port's LLDP TLV inclusion of System Capabilities.

sys-desc

    Display the port's LLDP TLV inclusion of System Description.

sys-name

    Display the port's LLDP TLV inclusion of System Name.
3.8.12 show lldp remote-data

This command shows all LLDP remote-data settings and states concerning one or all ports.

Format

```
show lldp remote-data <{slot/port|all}>
    chassis-id | detailed | ether-port-info | link-aggregation-info |
    mgmt-addr |                  |
    port-desc | port-id | summary | sys-desc | sys-name
```

Mode

Privileged EXEC and User EXEC

chassis-id

Display the remote data's chassis ID only.

detailed

Display remote data in detailed format (i.e., all available data). Note: most important data is output first (not in alphabetic order of command names). This is the default command if no specific command is given.

ether-port-info

Display the remote data's port Ethernet properties only (group command, outputs: Port Autoneg. Supported, Port Autoneg. Enabled, Port Autoneg. Advertized Capabilities and Port Operational MAU Type).

inlinenpower

Displays the remote port's Power over Ethernet capabilities (PoE, IEEE 802.3af). Included are if the remote device is a PSE (Power Source Device) or a PD (Powered Device), if PoE is supported and if the power pairs are selectable.

link-aggregation-info

Display the remote data's link aggregation information only (group command, outputs: Link Agg. Status and Link Agg. Port ID).

mgmt-addr

Display the remote data's management address only.
3.8 LLDP - Link Layer Discovery Protocol

**port-desc**
Display the port's LLDP TLV inclusion of Port Description.

**port-id**
Display the remote data's port ID only.

**summary**
Display remote data in summary format (table with most important data only, strings will be truncated if necessary, indicated by an appended '>' character).

**sys-desc**
Display the remote data's system description only.

**sys-name**
Display the remote data's system name only.

### 3.8.13 lldp
Enable/disable the LLDP/IEEE802.1AB functionality on this device. If disabled, the LLDP protocol will become inactive, but the LLDP MIBs can still be accessed. This command is a shorthand notation for `lldp config chassis admin-state {off|on}` (see “lldp config chassis admin-state” on page 169).

The default setting is on.

**Format**
```
lldp
```

**Mode**
Global Config
3.8 LLDP - Link Layer Discovery Protocol

### no lldp
Disable the LLDP/IEEE802.1AB functionality on this device.

**Format**

```plaintext
no lldp
```

**Mode**

```
Global Config
```

---

#### 3.8.14 lldp config chassis admin-state

Configure the LLDP/IEEE802.1AB functionality on this device. If disabled, the LLDP protocol will become inactive, but the LLDP MIBs can still be accessed.

- **off**: Disable the LLDP/IEEE802.1AB functionality.
- **on**: Enable the LLDP/IEEE802.1AB functionality.

The default setting is **on**.

**Format**

```plaintext
lldp config chassis admin-state {off|on}
```

**Mode**

```
Global Config
```
3.8.15 lldp config chassis notification-interval

Configure the LLDP minimum notification interval (the minimum time after a notification trap has been sent until a new trap can be sent, unit: seconds, min.: 5 sec., max.: 3600 sec., default: 5 sec.).

**Format**

```
lldp config chassis notification-interval <notification interval>
```

**Mode**

Global Config

**Notification interval**

Configure the LLDP minimum notification interval (the minimum time after a notification trap has been sent until a new trap can be sent, unit: seconds, min.: 5 sec., max.: 3600 sec., default: 5 sec.).

3.8.16 lldp config chassis re-init-delay

Configure the LLDP re-initialization delay (unit: seconds, min.: 1 sec., max.: 10 sec., default: 2 sec.).

**Format**

```
lldp config chassis re-init-delay <re-init delay>
```

**Mode**

Global Config

**Re-init-delay**

Configure the LLDP re-initialization delay (unit: seconds, min.: 1 sec., max.: 10 sec., default: 2 sec.).
3.8.17 lldp config chassis tx-delay

Configure the LLDP transmit delay, the delay between successive LLDP frame transmissions (unit: seconds, min.: 1 sec., max.: 8192 sec., default: 2 sec.).

Format

lldp config chassis tx-delay <tx delay>

Mode

Global Config

Tx-delay

Configure the LLDP transmit delay, the delay between successive LLDP frame transmissions (unit: seconds, min.: 1 sec., max.: 8192 sec., default: 2 sec.).

3.8.18 lldp config chassis tx-hold-mult

Configure the LLDP transmit hold multiplier, a time-to-live value expressed as a multiple of the LLDP Message Tx Interval (tx-interval), min.: 2, max.: 10, default: 4.

Format

lldp config chassis tx-hold-mult <tx hold multiplier>

Mode

Global Config

Tx-hold-mult

Configure the LLDP transmit hold multiplier, a time-to-live value expressed as a multiple of the LLDP Message Tx Interval (tx-interval), min.: 2, max.: 10, default: 4.
3.8.19 lldp config chassis tx-interval

Configure the interval at which LLDP frames are transmitted on behalf of this LLDP agent (unit: seconds, min.: 5 sec., max.: 32768 sec., default: 30 sec.)

Format

    lldp config chassis tx-interval <tx interval>

Mode

    Global Config

Tx-interval

    Configure the interval at which LLDP frames are transmitted on behalf of this LLDP agent (unit: seconds, min.: 5 sec., max.: 32768 sec., default: 30 sec.).

3.8.20 clear lldp config all

Clear the LLDP configuration, i. e., set all configurable parameters to default values (all chassis- as well as port-specific parameters at once).
Note: LLDP Remote data remains unaffected.

Format

    clear lldp config all

Mode

    Privileged EXEC
3.8.21 lldp admin-state

Configure the port's LLDP admin state (if LLDP/IEEE802.1AB frames will be transmitted to and/or received from the standard IEEE multicast address 01:80:c2:00:00:0e).

The default setting is `tx-and-rx`.

**Format**

```
lldp admin-state <{tx-only|rx-only|tx-and-rx|off}>
```

**Mode**

```
Interface Config
```

3.8.22 lldp fdb-mode

Configure the port's LLDP FDB mode.

The default setting is `autodetect`.

**Format**

```
lldp fdb-mode <{lldp-only|mac-only|lldp-and-mac|autodetect}>
```

**Mode**

```
Interface Config
```
3.8.23 lldp hm-mode

Configure the port's LLDP Hirschmann mode (if LLDP/IEEE802.1AB frames will be transmitted to and/or received from the Hirschmann-specific multicast address 01:80:63:2f:ff:0b).

The default setting is tx-and-rx.

Format

    lldp hm-mode <{tx-only|rx-only|tx-and-rx|off}>

Mode

    Interface Config

tx-only

    Port will only transmit LLDP frames but will not process received frames.

rx-only

    Port will not transmit any LLDP frames but will process received frames.

tx-and-rx

    Port will transmit LLDP frames and will also process received frames. This is the default setting.

off

    Port will neither transmit LLDP frames nor process received frames.

3.8.24 lldp max-neighbors

Configure the port's LLDP max. no. of neighbors (min.: 1, max.: 50, default: 10).

Format

    lldp max-neighbors <1..50>

Mode

    Interface Config
3.8.25 lldp notification
Configure the port's LLDP notification setting (on or off, default: off).

Format
    lldp notification {off|on}

Mode
    Interface Config

3.8.26 lldp tlv link-aggregation
Configure the port's LLDP TLV inclusion of Link Aggregation (on or off, default: on).

Format
    lldp tlv link-aggregation {off|on}

Mode
    Interface Config

3.8.27 lldp tlv mac-phy-config-state
Configure the port's LLDP TLV inclusion of MAC Phy. Cfg. State (on or off, default: on).

Format
    lldp tlv mac-phy-config-state {off|on}

Mode
    Interface Config
3.8.28 lldp tlv max-frame-size

Configure the port's LLDP TLV inclusion of Max. Frame Size (on or off, default: on).

Format
lldp tlv max-frame-size <{off|on}>

Mode
Interface Config

3.8.29 lldp tlv mgmt-addr

Configure the port's LLDP TLV inclusion of Management Address (on or off, default: on).

Format
lldp tlv mgmt-addr <{off|on}>

Mode
Interface Config

3.8.30 lldp tlv port-desc

Configure the port's LLDP TLV inclusion of Port Description (on or off, default: on).

Format
lldp tlv port-desc <{off|on}>

Mode
Interface Config
3.8.31 lldp tlv gmrp

Configure the port’s LLDP TLV inclusion of GMRP (on or off, default: on).

Format

    lldp tlv gmrp <{off|on (on)}>  

Mode

    Interface Config

3.8.32 lldp tlv igmp

Configure the port’s LLDP TLV inclusion of IGMP (on or off, default: on).

Format

    lldp tlv igmp <{off|on (on)}>  

Mode

    Interface Config

3.8.33 lldp tlv portsec

Configure the port’s LLDP TLV inclusion of PortSec (on or off, default: on).

Format

    lldp tlv portsec <{off|on (on)}>  

Mode

    Interface Config
### 3.8.34 lldp tlv ptp

Configure the port's LLDP TLV inclusion of PTP (on or off, default: on).

**Format**

```
lldp tlv ptp <{off|on (on)}>:
```

**Mode**

- Interface Config

### 3.8.35 lldp tlv protocol

Configure the port's LLDP TLV inclusion of Protocol (on or off, default: on).

**Format**

```
lldp tlv protocol <{off|on (on)}>:
```

**Mode**

- Interface Config

### 3.8.36 lldp tlv sys-cap

Configure the port's LLDP TLV inclusion of System Capabilities (on or off, default: on).

**Format**

```
lldp tlv sys-cap <{off|on}>:
```

**Mode**

- Interface Config
3.8.37 lldp tlv sys-desc
Configure the port's LLDP TLV inclusion of System Description (on or off, default: on).

**Format**
```
        lldp tlv sys-desc <{off|on}>
```

**Mode**
```
        Interface Config
```

3.8.38 lldp tlv sys-name
Configure the port's LLDP TLV inclusion of System Name (on or off, default: on).

**Format**
```
        lldp tlv sys-name <{off|on}>
```

**Mode**
```
        Interface Config
```

3.8.39 name
Set or remove a descriptive name for the current interface (physical ports only).

**Format**
```
        name <descriptive name>
```

**Mode**
```
        Interface Config
```
<descriptive name>

Enter a descriptive name for the current interface (physical ports only). Max. length is 20 characters.

Note: If it contains blanks or exclamation marks (!), enclose it in quotation marks ("). The description itself must not contain any quotation marks (" or "), question marks (?) or backslashes (\).

no name

Delete the descriptive name for the current interface (physical ports only).

Format

```
no name
```

Mode

Interface Config
3.9 SNTP - Simple Network Time Protocol

These commands show and configure the SNTP parameters.

3.9.1 show sntp

This command shows all SNTP settings.

Format

```
show sntp
```

Mode

Privileged EXEC and User EXEC

SNTP Server Anycast Address

Show SNTP Server Anycast Address (a.b.c.d).

SNTP Server Anycast Transmit Interval

Show SNTP Anycast Transmit Interval (in seconds).

SNTP Server Anycast VLAN

Show SNTP Server Anycast VLAN.

SNTP Server Disable if Timesource is local

Show SNTP Server Disable if Timesource is local (Yes/No).

SNTP Client Accepts Broadcasts

Show SNTP Client Accepts Broadcasts (Yes/No).

SNTP Client Disable after Synchronization

Show SNTP Client Disable after Synchronization (Yes/No).

SNTP Client Request Interval

Show SNTP Client Request Interval (in seconds).
SNTP Client Local Time Offset
Show SNTP Client Local Time Offset (in minutes).

SNTP Client Primary Server IP Address
Show SNTP Client Primary Server IP Address (a.b.c.d).

SNTP Client Secondary Server IP Address
Show SNTP Client Secondary Server IP Address (a.b.c.d).

SNTP Client Threshold to Server Time
Show SNTP Client Threshold to Server Time (in milliseconds).

SNTP Operation Global
Show SNTP Operation Global (Disabled or Enabled).

SNTP Operation Server
Show SNTP Operation Server (Disabled or Enabled).

SNTP Operation Client
Show SNTP Operation Client (Disabled or Enabled).

SNTP Status
Show SNTP Status

SNTP Time
Show SNTP Time (yyyy-mm-dd hh:mm:ss).

SNTP System Time
Show SNTP system Time (yyyy-mm-dd hh:mm:ss).

3.9.2 show sntp anycast
This command shows all SNTP anycast configuration settings.

Format
show sntp anycast [address|transmit-interval|vlan]

Mode
Privileged EXEC and User EXEC
address
Show the SNTP server's anycast destination IP Address.

transmit-interval
Show the SNTP Server's interval for sending Anycast messages (unit: seconds).

3.9.3 show sntp client
This command shows all SNTP anycast configuration settings.

Format
```
show sntp client [accept-broadcast|disable-after-sync|offset|request-interval|server<primary|secondary>|threshold]
```

Mode
Privileged EXEC and User EXEC

accept-broadcast
Show if the SNTP Client accepts SNTP broadcasts.

disable-after-sync
Show if the SNTP client will be disabled once it is synchronized to the time server.

offset
Show the local time's offset (in minutes) with respect to UTC (positive values for locations east of Greenwich).

request-interval
Show the SNTP Client's request interval (unit: seconds).

server
Show the SNTP Client's server IP addresses.
server primary
   Show the SNTP Client's primary server IP addresses.

server secondary
   Show the SNTP Client's redundant server IP addresses.

server threshold
   Show the SNTP Client's threshold in milliseconds.

3.9.4 show sntp operation
This command shows if the SNTP function is enabled or disabled.

Format
   show sntp operation

Mode
   Privileged EXEC and User EXEC

3.9.5 show sntp server
This command shows the SNTP Server's configuration parameters.

Format
   show sntp server [disable-if-local]

Mode
   Privileged EXEC and User EXEC

disable-if-local
   Show if the server will be disabled if the time is running from the local clock and not synchronized to an external time source.
3.9.6  show sntp status

This command shows the SNTP state, synchronization and error messages.

**Format**

```
show sntp status
```

**Mode**

Privileged EXEC and User EXEC

3.9.7  show sntp time

This command shows time and date.

**Format**

```
show sntp time [sntp|system]
```

**Mode**

Privileged EXEC and User EXEC

- **sntp**
  - Show the current SNTP date and UTC time.

- **system**
  - Show the local system's current date and time.
3.9.8  no sntp

This command disables sntp.

Format

    no sntp

Mode

    Global Config

3.9.9  sntp anycast address

Set the SNTP server's anycast destination IP Address, default: 0.0.0.0 (none).

Format

    sntp anycast address <IP-Address>

Mode

    Global Config

no sntp anycast address

Set the SNTP server's anycast destination IP Address to 0.0.0.0.

Format

    no sntp anycast address

Mode

    Global Config
3.9.10 snntp anycast transmit-interval

The transmit interval in seconds, default: 120.

Format

    sntp anycast transmit-interval <1-3600>

Mode

    Global Config

3.9.11 snntp client accept-broadcast

Enable/Disable that the SNTP Client accepts SNTP broadcasts.

Format

    sntp client accept-broadcast <on | off>

Mode

    Global Config

no snntp accept-broadcast

Disable the SNTP Client accepts SNTP broadcasts.

Format

    no snntp client accept-broadcast

Mode

    Global Config
3.9.12 sntp client disable-after-sync

If this option is activated, the SNTP client disables itself once it is synchronised to a server.

**Format**

```plaintext
sntp client disable-after-sync <on | off>
```

**Mode**

- **off**
  - Do not disable SNTP client when it is synchronised to a time server.
- **on**
  - Disable SNTP client as soon as it is synchronised to a time server.

3.9.13 sntp client offset

The offset between UTC and local time in minutes, default: 60.

**Format**

```plaintext
sntp client offset <-1000 to 1000>
```

**Mode**

- **Global Config**
3.9.14 sntp client request-interval

The synchronization interval in seconds, default: 30.

Format

    sntp client request-interval <1-3600>

Mode

    Global Config

3.9.15 no sntp client server

Disable the SNTP client servers.

Format

    no sntp client server

Mode

    Global Config

3.9.16 sntp client server primary

Set the SNTP Client's primary server IP Address, default: 0.0.0.0 (none).

Format

    sntp client server primary <IP-Address>

Mode

    Global Config
**3.9.17 snntp client server secondary**

Set the SNTP Client's secondary server IP Address, default: 0.0.0.0 (none).

**Format**
```
  snntp client server secondary <IP-Address>
```

**Mode**
- Global Config

**no snntp client server secondary**

Disable the secondary SNTP client server.

**Format**
```
  no snntp client server secondary
```

**Mode**
- Global Config
3.9.18 sntp client threshold

With this option you can reduce the frequency of time alterations. Enter this threshold as a positive integer value in milliseconds. The switch obtains the server timer as soon as the deviation to the server time is above this threshold.

**Format**

```
  sntp client threshold <milliseconds>
```

**Mode**

Global Config

**Milliseconds**

Enter the allowed deviation to the server time as a positive integer value in milliseconds.

- **no sntp client threshold**
  Disable the sntp client threshold.

**Format**

```
  no sntp client threshold
```

**Mode**

Global Config
3.9.19 sntp operation

Enable/Disable the SNTP function.

Format

```
sntp operation <on | off> |
  client { on | off } |
  server { on | off }
```

Mode

Global Config

client

Enable or disable SNTP Client.

server

Enable or disable SNTP Server.

no sntp operation

Disable the SNTP Client and Server.

Format

```
no sntp operation
```

Mode

Global Config
3.9.20 sntp server disable-if-local

With this option enabled, the switch disables the SNTP Server Function if it is not synchronized to a time server itself.

**Format**

```
sntp server disable-if-local <on | off>
```

**Mode**

- **off**
  
  Enable the SNTP Server even if it is not synchronized to a time server itself.

- **on**
  
  Disable the SNTP Server if it is not synchronized to a time server itself.

3.9.21 sntp time system

Set the current sntp time.

**Format**

```
sntp time system <YYYY-MM-DD HH:MM:SS>
```

**Mode**

- Global Config
3.10 PTP - Precision Time Protocol

These commands show and configure the PTP (IEEE 1588) parameters. The operation parameter is available for all devices. All other parameters are additionally available for MS20/MS30 and PowerMICE.

3.10.1 show ptp

This command shows all PTP settings.

Format

show ptp

Mode

Privileged EXEC and User EXEC

3.10.2 ptp clock-mode

Configure the Precision Time Protocol (PTP, IEEE 1588) clock mode. If the clock mode is changed, PTP will be initialized. The default is "disable"

Format

ptp clock-mode {v1-simple-mode | v2-simple-mode}

Mode

Global Config
v1-simple-mode

Set the clock mode to 'v1 Simple Mode'. This is a client only mode without hardware support. The device only accepts PTPv1 sync messages and sets the time directly. No BMC algorithm will run.

v2-simple-mode

Set the clock mode to 'v2 Simple Mode'. This is a client only mode without hardware support. The device only accepts PTPv2 sync (or follow_up) messages and sets the time directly. No BMC algorithm will run.

3.10.3 ptp operation

Enable or disable the Precision Time Protocol (IEEE 1588). The default is "disable"

Format

ptp operation {disable|enable}

Mode

Global Config

disable

Disable the Precision Time Protocol (IEEE 1588).

enable

Enable the Precision Time Protocol (IEEE 1588).
3.11 PoE - Power over Ethernet

These commands show and configure the Power over Ethernet (IEEE 802.3af) parameters.

PoE commands are available exclusively on ports which are located on modules supporting Power over Ethernet (PoE, IEEE 802.3af).

PoE is available for MACH 4000 and OCTOPUS devices with PoE modules.

3.11.1 show inlinepower

This command shows global Inline Power settings PoE.

Format

show inlinepower

Mode

Privileged EXEC and User EXEC

3.11.2 inlinepower (Global Config Mode)

Configure the global Inline Power parameters.

Format

inlinepower {admin-mode {disable|enable} | trap {disable|enable} | threshold <1-99> }

Mode

Global Config
admin-mode
Configure the global Inline Power administrative setting (enable or disable, default: enable).

trap
Configure the Inline Power notification (trap) setting (enable or disable, default: disable).

threshold
Configure the Inline Power notification (trap) threshold (unit: percent of maximum rated power, valid range: 1-99, default: 90).

3.11.3 inlinepower (Interface Config Mode)
Configure the port-related Inline Power parameters.
Note: The interface name you enter in the name-command.

Format
inlinepower {admin-mode {disable|enable} | priority {critical|high|low} }

Mode
Interface Config

admin-mode
Configure the port-related Inline Power administrative setting (enable or disable, default: enable).

priority
Configure the Inline Power priority for this port. In case of power scarcity, inline power on ports configured with the lowest priority is dropped first. Possible values are: critical, high or low, default: low. The highest priority is critical.
4 CLI Commands: Switching

This section provides detailed explanation of the Switching commands. The commands are divided into two functional groups:

- Show commands display spanning tree settings, statistics, and other information.
- Configuration Commands configure features and options of the switch. For every configuration command there is a show command that displays the configuration setting.
4.1 Spanning Tree Commands

4.1.1 show spanning-tree

This command displays spanning tree settings for the common and internal spanning tree, when the optional parameter “brief” is not included in the command. The following details are displayed.

Format

```
show spanning-tree [brief]
```

Mode

Privileged EXEC and User EXEC

Spanning Tree Adminmode

Enabled or Disabled

Bridge Priority

Configured value.

Bridge Identifier

The bridge identifier for the CST (CST = Classical Spanning Tree IEEE 802.1d). It is made up using the bridge priority and the base MAC address of the bridge.

Time Since Topology Change

in seconds

Topology Change Count

Number of times changed.

Topology Change

Boolean value of the Topology Change parameter for the switch indicating if a topology change is in progress on any port assigned to the common and internal spanning tree.

Designated Root

The bridge identifier of the root bridge. It is made up from the bridge priority and the base MAC address of the bridge.

Root Path Cost

Value of the Root Path Cost parameter for the common and internal spanning tree.
Root Port Identifier
Identifier of the port to access the Designated Root for the CST.

Root Port Max Age
Derived value

Root Port Bridge Forward Delay
Derived value

Hello Time
Configured value

Bridge Hold Time
Minimum time between transmission of Configuration Bridge Protocol Data Units (BPDUs)

CST Regional Root
Bridge Identifier of the CST Regional Root. It is made up using the bridge priority and the base MAC address of the bridge.

Regional Root Path Cost
Path Cost to the CST Regional Root.

Associated FIDs
List of forwarding database identifiers currently associated with this instance.

Associated VLANs
List of VLAN IDs currently associated with this instance.

**show spanning-tree brief**

When the “brief” optional parameter is included, this command displays a brief overview of the spanning tree settings for the bridge. In this case, the following details are displayed.

Bridge Priority
Configured value.

Bridge Identifier
The bridge identifier for the selected MST instance. It is made up using the bridge priority and the base MAC address of the bridge.
CLI Commands: Switching

4.1 Spanning Tree Commands

**Bridge Max Age**
Configured value.

**Bridge Hello Time**
Configured value.

**Bridge Forward Delay**
Configured value.

**Bridge Hold Time**
Minimum time between transmission of Configuration Bridge Protocol Data Units (BPDUs)

**Rstp Mrp Mode**
Rapid spanning tree mrp (Media Redundancy Protocol) mode (Enabled/Disabled)

**Rstp Mrp configuration error**
Configuration error in Rapid spanning tree mrp (Media Redundancy Protocol) (No/Yes)

### 4.1.2 show spanning-tree interface

This command displays the settings and parameters for a specific switch port within the common and internal spanning tree. The <slot/port> is the desired switch port. The following details are displayed on execution of the command.

**Format**
```
show spanning-tree interface <slot/port>
```

**Mode**
Privileged EXEC and User EXEC

**Port mode**
Enabled or disabled.
Port Up Time Since Counters Last Cleared
   Time since port was reset, displayed in days, hours, minutes, and seconds.

STP BPDUs Transmitted
   Spanning Tree Protocol Bridge Protocol Data Units sent

STP BPDUs Received
   Spanning Tree Protocol Bridge Protocol Data Units received.

RST BPDUs Transmitted
   Rapid Spanning Tree Protocol Bridge Protocol Data Units sent

RST BPDUs Received
   Rapid Spanning Tree Protocol Bridge Protocol Data Units received.

MSTP BPDUs Transmitted
   Multiple Spanning Tree Protocol Bridge Protocol Data Units sent

MSTP BPDUs Received
   Multiple Spanning Tree Protocol Bridge Protocol Data Units received.

4.1.3 show spanning-tree mst detailed

This command displays settings and parameters for the specified multiple spanning tree instance. The instance \(<\text{mstid}>\) is a number that corresponds to the desired existing multiple spanning tree instance ID. The following details are displayed.

Format
   show spanning-tree mst detailed \(<\text{mstid}>\)

Mode
   Privileged EXEC and User EXEC

mstid
   Enter a multiple spanning tree instance identifier.
   Valid values: 0 - 4094.
MST Instance ID
Valid value: 0

MST Bridge Priority
Valid values: 0-61440 in increments of 4096.

Time Since Topology Change
in seconds

Topology Change Count
Number of times the topology has changed for this multiple spanning tree instance.

Topology Change in Progress
Value of the Topology Change parameter for the multiple spanning tree instance.

Designated Root
Identifier of the Regional Root for this multiple spanning tree instance.

Root Path Cost
Path Cost to the Designated Root for this multiple spanning tree instance

Root Port Identifier
Port to access the Designated Root for this multiple spanning tree instance

Associated FIDs
List of forwarding database identifiers associated with this instance.

Associated VLANs
List of VLAN IDs associated with this instance.
4.1.4 show spanning-tree mst port detailed

This command displays the detailed settings and parameters for a specific switch port within a particular multiple spanning tree instance. The instance `<mstid>` is a number that corresponds to the desired existing multiple spanning tree instance. The `<slot/port>` is the desired switch port.

**Format**

```
show spanning-tree mst port detailed <mstid> <slot/port>
```

**Mode**

Privileged EXEC and User EXEC

**MST Instance ID**

Valid value: 0

**Port Identifier**

Port priority as a two digit hex number followed by the port number as a two digit hex number.

**Port Priority**

Decimal number.

**Port Forwarding State**

Current spanning tree state of this port

**Port Role**

The port’s current RSTP port role.

**Port Path Cost**

Configured value of the Internal Port Path Cost parameter

**Designated Root**

The Identifier of the designated root for this port.

**Designated Port Cost**

Path Cost offered to the LAN by the Designated Port

**Designated Bridge**

Bridge Identifier of the bridge with the Designated Port.

**Designated Port Identifier**

Port on the Designated Bridge that offers the lowest cost to the LAN
If 0 (defined as the default CIST ID) is passed as the <mstid>, then this command displays the settings and parameters for a specific switch port within the common and internal spanning tree. The <slot/port> is the desired switch port. In this case, the following are displayed.

**Port Identifier**
- The port identifier for this port within the CST.

**Port Priority**
- The priority of the port within the CST.

**Port Forwarding State**
- The forwarding state of the port within the CST.

**Port Role**
- The role of the specified interface within the CST.

**Port Path Cost**
- The configured path cost for the specified interface.

**Designated Root**
- Identifier of the designated root for this port within the CST.

**Designated Port Cost**
- Path Cost offered to the LAN by the Designated Port.

**Designated Bridge**
- The bridge containing the designated port.

**Designated Port Identifier**
- Port on the Designated Bridge that offers the lowest cost to the LAN.

**Topology Change Acknowledgement**
- Value of flag in next Configuration Bridge Protocol Data Unit (BPDU) transmission indicating if a topology change is in progress for this port.

**Hello Time**
- The hello time in use for this port.

**Edge Port**
- The configured value indicating if this port is an edge port.
Edge Port Status
The derived value of the edge port status. True if operating as an edge port; false otherwise.

Point To Point MAC Status
Derived value indicating if this port is part of a point to point link.

CST Regional Root
The regional root identifier in use for this port.

CST Port Cost
The configured path cost for this port.
4.1.5 show spanning-tree mst port summary

This command displays the settings of one or all ports within the specified multiple spanning tree instance. The parameter `<mstid>` indicates a particular MST instance. The parameter `{<slot/port> | all}` indicates the desired switch port or all ports.

If 0 (defined as the default CIST ID) is passed as the `<mstid>`, then the status summary is displayed for one or all ports within the common and internal spanning tree.

**Format**

```
show spanning-tree mst port summary <mstid> {<slot/port> | all}
```

**Mode**

Privileged EXEC and User EXEC

**MST Instance ID**

The MST instance associated with this port. Valid value: 0.

**Interface**

Valid slot and port number separated by forward slashes.

**STP Mode**

Current STP mode of this port in the specified spanning tree instance.

**Type**

Currently not used.

**Port Forwarding State**

The forwarding state of the port in the specified spanning tree instance

**Port Role**

The role of the specified port within the spanning tree.
4.1.6  **show spanning-tree summary**

This command displays spanning tree settings and parameters for the switch. The following details are displayed on execution of the command.

**Format**

```
show spanning-tree summary
```

**Mode**

Privileged EXEC and User EXEC

**Spanning Tree Adminmode**

Enabled or disabled.

**Spanning Tree Version**

Version of 802.1 currently supported (IEEE 802.1s, IEEE 802.1w, or IEEE 802.1d) based upon the Force Protocol Version parameter

**Configuration Name**

Configured name.

**Configuration Revision Level**

Configured value.

**Configuration Digest Key**

Calculated value.

**Configuration Format Selector**

Configured value.

**MST Instances**

List of all multiple spanning tree instances configured on the switch
4.1.7 show spanning-tree vlan

This command displays the association between a VLAN and a multiple spanning tree instance. The `<vlanid>` corresponds to an existing VLAN ID (1-4042).

**Format**

```
show spanning-tree vlan <vlanid>
```

**Mode**
Privileged EXEC and User EXEC

**vlanid**
Enter a VLAN identifier (1 - 4042).

**VLAN Identifier**
The VLANs associated with the selected MST instance.

**Associated Instance**
Identifier for the associated multiple spanning tree instance or "CST" if associated with the common and internal spanning tree.
4.1.8 spanning-tree

This command sets the spanning-tree operational mode to enabled.

Default
   disabled

Format
   spanning-tree

Mode
   Global Config

no spanning-tree

This command sets the spanning-tree operational mode to disabled. While disabled, the spanning-tree configuration is retained and can be changed, but is not activated.

Format
   no spanning-tree

Mode
   Global Config
4.1.9 spanning-tree auto-edgeport

This command specifies that this port is an Edge Port within the common and internal spanning tree. This will allow this port to transition to Forwarding State without delay.

**Format**

```
spanning-tree auto-edgeport
```

**Mode**

Interface Config

---

**no spanning-tree auto-edgeport**

This command specifies that this port is not an Edge Port within the common and internal spanning tree.

**Format**

```
no spanning-tree auto-edgeport
```

**Mode**

Interface Config
4.1.10 spanning-tree configuration name

This command sets the Configuration Identifier Name for use in identifying the configuration that this switch is currently using. The <name> is a string of at most 32 characters.

Default
The base MAC address displayed using hexadecimal notation as specified in IEEE 802 standard.

Format
spanning-tree configuration name <name>

Mode
Global Config

no spanning-tree configuration name
This command resets the Configuration Identifier Name to its default.

Format
no spanning-tree configuration name

Mode
Global Config
4.1.11 `spanning-tree configuration revision`

This command sets the Configuration Identifier Revision Level for use in identifying the configuration that this switch is currently using. The Configuration Identifier Revision Level is a number in the range of 0 to 65535.

Default

0

Format

`spanning-tree configuration revision <0-65535>`

Mode

Global Config

**no spanning-tree configuration revision**

This command sets the Configuration Identifier Revision Level for use in identifying the configuration that this switch is currently using to the default value, i.e. 0.

Format

`no spanning-tree configuration revision`

Mode

Global Config
4.1.12 spanning-tree edgeport

This command specifies that this port is an Edge Port within the common and internal spanning tree. This will allow this port to transition to Forwarding State without delay.

**Format**

```
spanning-tree edgeport
```

**Mode**

Interface Config

**no spanning-tree edgeport**

This command specifies that this port is not an Edge Port within the common and internal spanning tree.

**Format**

```
no spanning-tree edgeport
```

**Mode**

Interface Config
### 4.1.13 spanning-tree forceversion

This command sets the Force Protocol Version parameter to a new value. The Force Protocol Version can be one of the following:

- **802.1d** - ST BPDUs are transmitted (IEEE 802.1d functionality supported)
- **802.1w** - RST BPDUs are transmitted (IEEE 802.1w functionality supported)

**Default**

802.1w

**Format**

```
spanning-tree forceversion <802.1d | 802.1w>
```

**Mode**

Global Config

---

**no spanning-tree forceversion**

This command sets the Force Protocol Version parameter to the default value, i.e. 802.1w.

**Format**

```
no spanning-tree forceversion
```

**Mode**

Global Config
### 4.1.14 spanning-tree forward-time

This command sets the Bridge Forward Delay parameter to a new value for the common and internal spanning tree. The forward-time value is in seconds within a range of 4 to 30, with the value being greater than or equal to 
"(Bridge Max Age / 2) + 1".

**Default**

15

**Format**

```text
spanning-tree forward-time <4-30>
```

**Mode**

Global Config

---

#### no spanning-tree forward-time

This command sets the Bridge Forward Delay parameter for the common and internal spanning tree to the default value, i.e. 15.

**Format**

```text
no spanning-tree forward-time
```

**Mode**

Global Config
4.1.15 spanning-tree hello-time

This command sets the Hello Time parameter to a new value for the common and internal spanning tree. The hellotime <value> is in whole seconds within a range of 1 to 2 with the value being less than or equal to "(Bridge Max Age / 2) - 1".

**Default**

2

**Format**

```
spanning-tree hello-time <1-2>
```

**Mode**

- Interface Config
- Global Config

**no spanning-tree hello-time**

This command sets the Hello Time parameter for the common and internal spanning tree to the default value, i.e. 2.

**Format**

```
no spanning-tree hello-time
```

**Mode**

- Interface Config
- Global Config
4.1.16  **spanning-tree max-age**

This command sets the Bridge Max Age parameter to a new value for the common and internal spanning tree. The max-age value is in seconds within a range of 6 to 40, with the value being less than or equal to "2 times (Bridge Forward Delay - 1)".

**Default**

20

**Format**

`spanning-tree max-age <6-40>`

**Mode**

Global Config

---

**no spanning-tree max-age**

This command sets the Bridge Max Age parameter for the common and internal spanning tree to the default value, i.e. 20.

**Format**

`no spanning-tree max-age`

**Mode**

Global Config
### 4.1.17 spanning-tree max-hops

This command sets the Bridge Max Hops parameter to a new value for the common and internal spanning tree. The max-hops value is an integer within a range of 1 to 127.

**Format**

```
spanning-tree max-hops <1-127>
```

**Mode**

Global Config

---

**no spanning-tree max-hops**

This command sets the Bridge Max Hops parameter for the common and internal spanning tree to the default value, i.e. 20.

**Format**

```
no spanning-tree max-age
```

**Mode**

Global Config
4.1.18 spanning-tree mst

This command sets the Path Cost or Port Priority for this port within the multiple spanning tree instance or in the common and internal spanning tree. If the \texttt{<mstid>} parameter corresponds to an existing multiple spanning tree instance, then the configurations are done for that multiple spanning tree instance. If however 0 (defined as the default CIST ID) is passed as the \texttt{<mstid>}, then the configurations are performed for the common and internal spanning tree instance.

This command accepts the value 0 for the mstid, meaning the common and internal spanning tree.

If the 'cost' token is specified, this command sets the path cost for this port within a multiple spanning tree instance or the common and internal spanning tree instance, depending on the \texttt{<mstid>} parameter. The pathcost can be specified as a number in the range of 1 to 200000000 or auto. If "auto" is specified, the pathcost value will be set based on Link Speed.

If the 'port-priority' token is specified, this command sets the priority for this port within a specific multiple spanning tree instance or the common and internal spanning tree instance, depending on the \texttt{<mstid>} parameter. The port-priority value is a number in the range of 0 to 240 in increments of 16.

Default

\begin{verbatim}
  cost : auto; external-cost : auto;
  port-priority : 128
\end{verbatim}

Format

\begin{verbatim}
spanning-tree mst <mstid>
  {cost <1-200000000> | auto } |
  {external-cost <1-200000000> | auto } |
  port-priority <0-240>
\end{verbatim}

Mode

Interface Config
no spanning-tree mst

This command sets the Path Cost or Port Priority for this port within the multiple spanning tree instance or in the common and internal spanning tree to the respective default values. If the <mstid> parameter corresponds to an existing multiple spanning tree instance, then the configurations are done for that multiple spanning tree instance. If however 0 (defined as the default CIST ID) is passed as the <mstid>, then the configurations are performed for the common and internal spanning tree instance.

This command accepts the value 0 for the mstid, meaning the common and internal spanning tree.

If the 'cost' token is specified, this command sets the path cost for this port within a multiple spanning tree instance or the common and internal spanning tree instance, depending on the <mstid> parameter, to the default value, i.e. a pathcost value based on the Link Speed.

If the 'port-priority' token is specified, this command sets the priority for this port within a specific multiple spanning tree instance or the common and internal spanning tree instance, depending on the <mstid> parameter, to the default value, i.e. 128.

Format

   no spanning-tree mst <mstid> <cost | port-priority>

Mode

   Interface Config
4.1.19 spanning-tree mst priority

This command sets the bridge priority for a specific multiple spanning tree instance. The instance <mstid> is a number that corresponds to the desired existing multiple spanning tree instance. The priority value is a number within a range of 0 to 61440 in increments of 4096. This command accepts the value 0 for the mstid.

If 0 (defined as the default CIST ID) is passed as the <mstid>, then this command sets the Bridge Priority parameter to a new value for the common and internal spanning tree. The bridge priority value again is a number within a range of 0 to 61440. The twelve least significant bits will be masked according to the 802.1s specification. This will cause the priority to be rounded down to the next lower valid priority.

Default
32768

Format
spanning-tree mst priority <mstid> <0-61440>

Mode
Global Config

no spanning-tree mst priority

This command sets the bridge priority for a specific multiple spanning tree instance to the default value, i.e. 32768. The instance <mstid> is a number that corresponds to the desired existing multiple spanning tree instance.

This command accepts the value 0 for the mstid.
If 0 (defined as the default CIST ID) is passed as the <mstid>, then this command sets the Bridge Priority parameter for the common and internal spanning tree to the default value, i.e. 32768.

Format
spanning-tree mst priority <mstid>

Mode
Global Config
4.1.20 spanning-tree mst vlan

This command adds an association between a multiple spanning tree instance and a VLAN. The VLAN will no longer be associated with the common and internal spanning tree. The instance <mstid> is a number that corresponds to the desired existing multiple spanning tree instance. The <vlanid> corresponds to an existing VLAN ID (1-4042). This command accepts the value 0 for the mstid.

Format

    spanning-tree mst vlan <mstid> <vlanid>

Mode

    Global Config

no spanning-tree mst vlan

This command removes an association between a multiple spanning tree instance and a VLAN. The VLAN will again be associated with the common and internal spanning tree. The instance <mstid> is a number that corresponds to the desired existing multiple spanning tree instance. The <vlanid> corresponds to an existing VLAN ID. This command accepts the value 0 for the mstid.

Format

    no spanning-tree mst vlan <mstid> <vlanid>

Mode

    Global Config
4.1.21 spanning-tree port mode

This command sets the Administrative Switch Port State for this port to enabled.

Default

disabled

Format

spanning-tree port mode

Mode

Interface Config

no spanning-tree port mode

This command sets the Administrative Switch Port State for this port to disabled.

Format

no spanning-tree port mode

Mode

Interface Config
4.1.22 spanning-tree port mode all

This command sets the Administrative Switch Port State for all ports to enabled.

**Default**

disabled

**Format**

spanning-tree port mode all

**Mode**

Global Config

---

**no spanning-tree port mode all**

This command sets the Administrative Switch Port State for all ports to disabled.

**Format**

no spanning-tree port mode all

**Mode**

Global Config
4.1.23 spanning-tree stp-mrp-mode

This command sets the spanning tree mrp (Media Redundancy Protocol) mode to enabled.

Default
disabled

Format
spanning-tree stp-mrp-mode

Mode
Global Config

no spanning-tree stp-mrp-mode

This command sets the spanning tree mrp (Medium Redundancy Protocol) mode to disabled.

Format
no spanning-tree stp-mrp-mode

Mode
Global Config
# 4.2 MRP

The concept of the MRP-Ring enables the construction of high-availability, ring-shaped network structures.

The two ends of a backbone in a line-type configuration can be closed to form a redundant ring - the MRP-Ring - by using the RM function (Redundancy Manager) of the Switch.

It is possible to mix the devices that support this function in any combination within the MRP ring.

If a line section becomes inoperable, the ring structure of up to 50 switches typically transforms back to a line-type configuration within 150 ms (maximum 500 ms).

## 4.2.1 show mrp

This command displays the settings and states of the MRP-Ring. The following details are displayed on execution of the command.

**Format**

```
show mrp [current-domain]
```

**Mode**

Privileged EXEC and User EXEC

**current-domain**

Specify the optional keyword "current-domain" to show the current MRP domain's settings. If you omit the keyword "current-domain", the show command will display the settings of all existing MRP domains. Note: currently, it is only possible to configure one MRP domain, so the keyword keyword "current-domain" can be omitted (it exists for future compatibility reasons).
4.2.2 show mrp current-domain

This command displays the settings and states of the MRP-Ring’s current domain. The following details are displayed on execution of the command. If you omit the optional keywords (e.g., advanced-mode), all settings will be displayed.

Format

```
show mrp current-domain [advanced-mode | domain-id | info | manager-priority | mode | name | recovery-delay | operation | port [primary | secondary] | summary]
```

Mode

Privileged EXEC and User EXEC

**advanced mode**

Show the switch's advanced mode setting for the given MRP domain.

**domain-id**

Show the given MRP domain's ID.

**info**

Show status information for the given MRP domain. Note: the information displayed depends on the switch's mode (Client or Manager) because only a subset of them are useful for each mode.

**manager-priority**

Show the switch's manager priority for the given MRP domain.

**mode**

Show the switch's mode for the given MRP domain.

**name**

Show the given MRP domain's name.

**recovery-delay**

Show the given MRP domain's recovery delay.

**operation**

Show the switch's administrative setting for the given MRP domain (enabled or disabled).

**port**

Show the ports for the given MRP domain
port primary
    Show the primary port for the given MRP domain.

port secondary
    Show the secondary port for the given MRP domain.

summary
    Show a summary for the given MRP domain.

4.2.3 mrp current-domain

Specify that you want to configure the current MRP domain's settings.

Default
    none

Format
    mrp current-domain {advanced-mode {disable|enable}
    | name <domain-name>
    | recovery-delay {500ms|200ms}
    | operation {disable|enable}
    | port {primary|secondary} <slot/port>

Mode
    Global Config

advanced-mode
    Enable or disable the switch's advanced mode for the given MRP domain.

manager-priority
    Configure the given MRP domain's manager priority (0-65535).

mode
    Configure the switch's MRP mode for the given domain (client or manager).
    client: Switch is client for the given MRP domain.
    manager: Switch is manager for the given MRP domain.
name
Set a name for the given MRP domain.

recovery-delay
Configure the MRP recovery delay for the given domain.
500ms: Recovery delay is 500 ms for the given MRP domain.
200ms: Recovery delay is 200 ms for the given MRP domain.

operation
Enable or disable the switch for the given MRP domain.

port
Specify the switch's ports for the given MRP domain (in slot/port notation).
primary: Specify the switch's primary port for the given MRP domain.
secondary: Specify the switch's secondary port for the given MRP domain.

4.2.4 mrp delete-domain
Delete current MRP domain.

Format
mrp delete-domain current-domain

Mode
Global Config
4.2.5  mrp new-domain

Create a new MRP domain. The configuration will consist of default parameters and its operation will be disabled.

Default
n/a not set

Format
mrp new-domain (<domain-id> | default-domain)

Mode
Global Config
domain-id
Enter a new MRP domain id. Format: 16 bytes in decimal notation, example: 1.2.3.4.5.6.7.8.9.10.11.12.13.14.15.16
The MRP domain id 0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0 is invalid.
default-domain
Create a default MRP domain (ID: 255.255.255.255.255.255.255.255.255.255.255.255.255.255.255.255).
4.3 HIPER-Ring

The concept of the HIPER-Ring enables the construction of high-availability, ring-shaped network structures. Within such a ring topology, network components supporting the HIPER-Ring are connected with each other via their ring ports. Exactly one redundancy manager assumes control of the ring. These commands are for configuring the Hirschmann High Performance Redundancy Ring.

Further information concerning this function you will find in the User Manual "Redundancy Configuration".
### 4.3.1 show hiper-ring

This command displays the settings and states of the HIPER-Ring. The following details are displayed on execution of the command.

**Format**
```
show hiper-ring
   {info | mode | port [primary | secondary] |
    redundancy-state | rm-state | recovery-delay}
```

**Mode**
- Privileged EXEC and User EXEC

**info**
Display the information about the HIPER-Ring configuration (cabling).

**mode**
Display the HIPER-Ring mode settings.

**port**
Display the HIPER-Ring's primary and secondary port properties.

**port primary**
Display the HIPER Ring's primary port properties.

**port secondary**
Display the HIPER Ring's secondary port properties.

**redundancy-state**
Display the actual state of the HIPER-Ring redundancy.

**rm-state**
Display the state of the HIPER Ring redundancy manager.

**recovery-delay**
Display the value of the recovery delay.
4.3.2 hiper-ring

Configure the HIPER-Ring.
Press Enter for a list of valid commands and their recommended order.

**Format**

```plaintext
hiper-ring
```

**Mode**

Global Config

---

**no hiper-ring**

Clear the HIPER Ring configuration (delete it).

**Format**

```plaintext
no hiper-ring
```

**Mode**

Global Config
4.3.3 hiper-ring mode

This command sets the HIPER-Ring mode. Possible values are:

- **ring-manager** Set the switch's HIPER Ring mode to Ring Manager.
- **rm** Abbreviation of Ring Manager.
- **ring-switch** Set the switch's HIPER Ring mode to Ring Switch.
- **rs** Abbreviation of Ring Switch.

**Default**
none

**Format**

```
hiper-ring mode <ring-switch|rs>
```

**Mode**
Global Config

4.3.4 hiper-ring port primary

Enter the switch's primary HIPER Ring port.

**Default**

```
n/a (not set)
```

**Format**

```
hiper-ring port primary <primary ring port>
```

**Mode**
Global Config

**primary ring port**

Enter the switch's primary HIPER Ring port (`<slot/port>`).
4.3.5 **hiper-ring port secondary**

Enter the switch's secondary HIPER Ring port.

**Default**

n/a not set

**Format**

`hiper-ring port secondary <secondary ring port>`

**Mode**

Global Config

**secondary ring port**

Enter the switch's secondary HIPER Ring port (`<slot/port>`).

4.3.6 **hiper-ring recovery-delay**

Defines the maximum recovery delay of ring recovery in the HIPER Ring (500 or 300 ms).

**Default**

n/a not set

**Format**

`hiper-ring recovery-delay (<500/300>)`

**Mode**

Global Config
4.4 DHCP Relay Commands

These commands configure the DHCP Relay parameters. The commands are divided by functionality into these different groups:

- **Configuration Commands** are used to configure features and options of the switch. For every configuration command there is a show command that will display the configuration setting.
- **Show commands** are used to display switch settings, statistics and other information.
- **Commands that start with the keyword 'no'** (so-called 'no commands') are used to clear some or all of the settings to factory defaults.

### 4.4.1 show dhcp-relay

Display the settings of the BOOTP/DHCP relay.

**Format**

```
show dhcp-relay [opt82 | port {<slot/port>|all} | server-address]
```

**Mode**

Privileged EXEC and User EXEC
4.4.2 dhcp-relay (Global Config Mode)

Set different options for BOOTP/DHCP relay and option 82 inclusion.

Format

dhcp-relay
{opt82
  {operation {disable|enable}| man-id <Manual Remote ID>|
   remote-id-type {client-id|ip|mac|other}}|
  server-address <Server-ID (1..4)> <Server IP Address>}

Mode

Global Config

dhcp-relay opt82 operation {disable|enable}
  Enable/Disable option 82 globally. Default: enable.

dhcp-relay opt82 man-id <Manual Remote ID>
  Configure the DHCP Relay's Option 82 Manual Value for the Remote
  ID Type (only effective, if Remote ID is set to "other"). Default: no ID.

dhcp-relay opt82 remote-id-type {client-id|ip|mac|other}
  Configure the DHCP Relay's Option 82 Remote ID Type.
  Default: mac

dhcp-relay server-address <Server ID (1..4)> <Server IP Address>
  Set the server IP address for one of the 4 possible server IDs.
  Default: 0.0.0.0

no dhcp-relay
  Clear the DHCP Relay configuration (set all server addresses to 0.0.0.0).

Format

  no dhcp-relay

Mode

  Global Config
4.4.3 dhcp-relay (Interface Config Mode)

Set different port specific options for option 82 inclusion.

Format

```
dhcp-relay {operation {disable|enable} | hirschmann-device {disable|enable} | hirschmann-agent {disable|enable}}
```

Mode

```
Interface Config
```

**dhcp-relay operation {disable|enable}**

Enable or disable the DHCP Relay's Option 82 on this port. Default: enable.

**dhcp-relay hirschmann-device {disable|enable}**

Enable this parameter if a Hirschmann DHCP client is connected to this port.
- It disables the forwarding of DHCP multicast requests that are received on this port.
- It will send its own DHCP multicast requests to be relayed by the DHCP relay; this will reduce the load in your network.

Disable this parameter if a Non-Hirschmann DHCP client is connected to this port (these devices send normal broadcast DHCP requests; this enables the relaying of DHCP broadcast requests that are received on this port).

**dhcp-relay hirschmann-agent {disable|enable}**

Enable or disable the forwarding of DHCP requests that are received on this port. Enable this parameter if a Hirschmann DHCP client is connected to this port. Default: disable.

Disable this parameter if a Non-Hirschmann DHCP client is connected to this port (these devices send normal broadcast DHCP requests; this enables the relaying of DHCP broadcast requests that are received on this port)

Enable this parameter if a Hirschmann DHCP client is connected to this port (it will send its own DHCP multicast requests to be relayed by the DHCP relay; this will reduce the load in your network).
This chapter provides a detailed explanation of the Security commands. The following Security CLI commands are available in the software Switching Package. Use the security commands to configure security settings for login users and port users.

The commands are divided into these different groups:

- **Show commands** are used to display device settings, statistics and other information.
- **Configuration Commands** are used to configure features and options of the switch. For every configuration command there is a show command that will display the configuration setting.
5.1 Security Commands

5.1.1 authentication login

This command creates an authentication login list. The <listname> is up to 15 alphanumeric characters and is not case sensitive. Up to 10 authentication login lists can be configured on the switch. When a list is created, the authentication method “local” is set as the first method.

When the optional parameters “Option1”, “Option2” and/or “Option3” are used, an ordered list of methods are set in the authentication login list. If the authentication login list does not exist, a new authentication login list is first created and then the authentication methods are set in the authentication login list. The maximum number of authentication login methods is three. The possible method values are local, radius and reject.

The value of local indicates that the user’s locally stored ID and password are used for authentication. The value of radius indicates that the user’s ID and password will be authenticated using the RADIUS server. The value of reject indicates the user is never authenticated.

To authenticate a user, the authentication methods in the user’s login will be attempted in order until an authentication attempt succeeds or fails.

Note: The default login list included with the default configuration can not be changed.

Note: When assigning a list to the 'admin' account, include an authentication method that allows administrative access even when remote authentication is unavailable.

Format

```
authentication login <listname> [method1 [method2 [method3]]]
```

Mode

Global Config
no authentication login

This command deletes the specified authentication login list. You will be unable to delete if any of the following conditions are true:

- The login list name is invalid or does not match an existing authentication login list
- The specified authentication login list is assigned to any user or to the non configured user for any component
- The login list is the default login list included with the default configuration and was not created using ‘authentication login’. The default login list cannot be deleted.

Format

no authentication login <listname>

Mode

Global Config
5.1.2 show authentication

This command displays the ordered authentication methods for all authentication login lists.

Format

    show authentication [users <listname>]

Mode

    Privileged EXEC and User EXEC

<listname>

- Enter the name of an existing Authentication List.
- Note: when assigning a list to the 'admin' account, include an authentication method that allows administrative access even when remote authentication is unavailable (use 'authentication login <listname>[method1 [method2 [method3]]]').

Authentication Login List

- This displays the authentication login listname.

Method 1

- This displays the first method in the specified authentication login list, if any.

Method 2

- This displays the second method in the specified authentication login list, if any.

Method 3

- This displays the third method in the specified authentication login list, if any.
5.1.3  show authentication users

This command displays information about the users assigned to the specified authentication login list. If the login is assigned to non-configured users, the user “default” will appear in the user column.

Format

    show authentication users <listname>

Mode

    Privileged EXEC and User EXEC

User

    This field displays the user assigned to the specified authentication login list.

Component

    This field displays the component (User or 802.1X) for which the authentication login list is assigned.
5.1.4 show users authentication

This command displays all user and all authentication login information. It also displays the authentication login list assigned to the default user.

**Format**

```
show users authentication
```

**Mode**

Privileged EXEC

**User**

This field lists every user that has an authentication login list assigned.

**System Login**

This field displays the authentication login list assigned to the user for system login.

**802.1x Port Security**

This field displays the authentication login list assigned to the user for 802.1X port security.
5.1.5 users login

This command assigns the specified authentication login list to the specified user for system login. The <user> must be a configured <user> and the <listname> must be a configured login list.

If the user is assigned a login list that requires remote authentication, all access to the interface from all CLI and web sessions will be blocked until the authentication is complete.

Note that the login list associated with the ‘admin’ user can not be changed to prevent accidental lockout from the switch.

Format

users login <user> <listname>

Mode

Global Config

user

Enter user name.

listname

Enter an alphanumeric string of not more than 15 characters.

Note: when assigning a list to the 'admin' account, include an authentication method that allows administrative access even when remote authentication is unavailable (use 'authentication login <listname> [method1 [method2 [method3]]]').
5.2 HTTP Commands

5.2.1 ip http server

This command enables access to the switch through the Web interface. When access is enabled, the user can login to the switch from the Web interface. When access is disabled, the user cannot login to the switch's Web server.

Disabling the Web interface takes effect immediately. All interfaces are effected.

Default
   enabled

Format
   ip http server

Mode
   Privileged EXEC

no ip http server

This command disables access to the switch through the Web interface. When access is disabled, the user cannot login to the switch's Web server.

Format
   no ip http server

Mode
   Privileged EXEC
6 Glossary

Numerics

802.1D. The IEEE designator for Spanning Tree Protocol (STP). STP, a link management protocol, is part of the 802.1D standard for media access control bridges. Using the spanning tree algorithm, STP provides path redundancy while preventing endless loops in a network. An endless loop is created by multiple active paths between stations where there are alternate routes between hosts. To establish path redundancy, STP creates a logical tree that spans all of the switches in an extended network, forcing redundant paths into a standby, or blocked, state. STP allows only one active path at a time between any two network devices (this prevents the loops) but establishes the redundant links as a backup if the initial link should fail. If STP costs change, or if one network segment in the STP becomes unreachable, the spanning tree algorithm reconfigures the spanning tree topology and reestablishes the link by activating the standby path. Without spanning tree in place, it is possible that both connections may be simultaneously live, which could result in an endless loop of traffic on the LAN.

802.1P. The IEEE protocol designator for Local Area Network (LAN). This Layer 2 network standard improves support of time critical traffic, and limits the extent of high bandwidth multicast traffic within a bridged LAN. To do this, 802.1P defines a methodology for introducing traffic class priorities. The 802.1P standard allows priority to be defined in all 802 MAC protocols (Ethernet, Token Bus, Token Ring), as well as in FDDI. For protocols (such as Ethernet) that do not contain a priority field, 802.1P specifies a method for indicating frame priority based on the new fields defined in the 802.1Q (VLAN) standard.

802.1Q VLAN. The IEEE protocol designator for Virtual Local Area Network (VLAN). This standard provides VLAN identification and quality of service (QoS) levels. Four bytes are added to an Ethernet frame to allow eight priority levels (QoS) and to identify up to 4096 VLANs. See “VLAN” on page 266 for more information.

A

Address Resolution Protocol. An Internet Protocol that dynamically maps Internet addresses to physical (hardware) addresses on a LAN.

Aging. When an entry for a node is added to the lookup table of a switch, it is given a timestamp. Each time a packet is received from a node, the timestamp is updated. The switch has a user-configurable timer that erases the entry after a certain length of time with no activity from that node.

Application Programming Interface. An API is an interface used by a programmer to interface with functions provided by an application.

AVL tree. Binary tree having the property that for any node in the tree, the difference in height between the left and right subtrees of that node is no more than 1.

B

BPDU. See “Bridge Protocol Data Unit” on page 256.


Bootstrap Protocol. An Internet protocol that enables a diskless workstation to discover its own IP address, the IP address of a BootP server on the network, and a file to be loaded into memory to boot the machine. This enables the workstation to boot without requiring a hard or floppy disk drive.

Bridge Protocol Data Unit. BPDU is the IEEE 802.1D MAC Bridge Management protocol that is the standard implementation of STP (Spanning Tree Protocol). It uses the STP algorithm to insure that physical loops in the network topology do not result in logical looping of network traffic. Using one bridge configured as root for reference, the BPDU switches one of two bridges forming a network loop into standby mode, so that only one side of a potential loop passes traffic. By examining frequent 802.1d configuration updates, a bridge in the standby mode can switch automatically into the forward mode if the other bridge forming the loop fails.

C

Checksum. A simple error-detection scheme in which each transmitted message is identified with a numerical value based on the number of set bits in the message. The receiving station then applies a formula to the message and checks to make sure the accompanying numerical value is the same. If not, the receiver can assume that the message has been corrupted.

CLI. See “Command Line Interface” on page 256.

Command Line Interface. CLI is a line-item interface for configuring systems.

Complex Programmable Logic Device. CPLD is a programmable circuit on which a logic network can
be programmed after its construction.

**CPLD.** See “Complex Programmable Logic Device.” on page 256.

**D**

**DHCP.** See “Dynamic Host Configuration Protocol.” on page 257.

**Differentiated Services.** Diffserv is a protocol for specifying and controlling network traffic by class so that certain types of traffic get precedence - for example, voice traffic, which requires a relatively uninterrupted flow of data, might get precedence over other kinds of traffic. Differentiated Services is the most advanced method for managing traffic in terms of what is called Class of Service (CoS). Unlike the earlier mechanisms of 802.1P tagging and Type of Service (ToS), Differentiated Services avoids simple priority tagging and depends on more complex policy or rule statements to determine how to forward a given network packet. An analogy is made to travel services, in which a person can choose among different modes of travel - train, bus, airplane - degree of comfort, the number of stops on the route, standby status, the time of day or period of year for the trip, and so forth. For a given set of packet travel rules, a packet is given one of 64 possible forwarding behaviors - known as per hop behaviors (PHBs). A six-bit field, known as the Differentiated Services Code Point (DSCP), in the Internet Protocol (Internet Protocol) header specifies the per hop behavior for a given flow of packets. Differentiated Services and the Class of Service approach provide a way to control traffic that is both more flexible and more scalability than the Quality of Service approach.

**Diffserv.** See “Differentiated Services.” on page 257.

**Dynamic Host Configuration Protocol.** DHCP is a protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. In some systems, the device's IP address can even change while it is still connected. DHCP also supports a mix of static and dynamic IP addresses. Dynamic addressing simplifies network administration because the software tracks IP addresses rather than requiring an administrator to manage the task. A new computer can be added to a network without the hassle of manually assigning it a unique IP address.

**E**

**EEPROM.** See “Electronically Erasable Programmable Read Only Memory” on page 258.
Electronically Erasable Programmable Read Only Memory. EEPROM is also known as Flash memory. This is reprogrammable memory.

F

FIFO. First In First Out.

Flash Memory. See “EEPROM” on page 257.

Flow Control. The process of adjusting the flow of data from one network device to another to ensure that the receiving device can handle all of the incoming data. This is particularly important where the sending device is capable of sending data much faster than the receiving device can receive it. There are many flow control mechanisms. One of the most common flow control protocols for asynchronous communication is called xon-xoff. In this case, the receiving device sends a “xoff” message to the sending device when its buffer is full. The sending device then stops sending data. When the receiving device is ready to receive more data, it sends an “xon” signal.

Forwarding. When a frame is received on an input port on a switch, the address is checked against the lookup table. If the lookup table has recorded the destination address, the frame is automatically forwarded on an output port.

Frame Check Sequence. The extra characters added to a frame for error detection and correction. FCS is used in X.25, HDLC, Frame Relay, and other data link layer protocols.

G


GARP Information Propagation.

GARP Multicast Registration Protocol. GMRP provides a mechanism that allows Bridges and end stations to dynamically register (and subsequently, de-register) Group membership information with the MAC Bridges attached to the same LAN segment, and for that information to be disseminated across all Bridges in the Bridged LAN that support Extended Filtering Services. The operation of GMRP relies upon the services provided by the GARP.

GARP VLAN Registration Protocol. GVRP allows workstations to request admission to a particular VLAN for multicast purposes.

GE. See “Gigabit Ethernet” on page 259.
Generic Attribute Registration Protocol. GARP provides a generic attribute dissemination capability that is used by participants in GARP Applications (called GARP Participants) to register and de-register attribute values with other GARP Participants within a Bridged LAN. The definition of the attribute types, the values that they can carry, and the semantics that are associated with those values when registered are specific to the operation of the GARP Application concerned.

Gigabit Ethernet. A high-speed Ethernet connection.

GMRP. See “GARP Multicast Registration Protocol” on page 258.

GVRP. See “GARP VLAN Registration Protocol.” on page 258.

H

hop count. The number of routers that a data packet passes through on its way to its destination.

I

ICMP. See “Internet Control Message Protocol” on page 259.

IGMP. See “Internet Group Management Protocol” on page 259.

IGMP Snooping. A series of operations performed by intermediate systems to add logic to the network to optimize the flow of multicast traffic; these intermediate systems (such as Layer 2 switches) listen for IGMP messages and build mapping tables and associated forwarding filters, in addition to reducing the IGMP protocol traffic. See “Internet Group Management Protocol” on page 259 for more information.

Internet Control Message Protocol. ICMP is an extension to the Internet Protocol (IP) that supports packets containing error, control, and informational messages. The PING command, for example, uses ICMP to test an Internet connection.

Internet Group Management Protocol. IGMP is the standard for IP Multicasting on the Internet. IGMP is used to establish host memberships in particular multicast groups on a single network. The mechanisms of the protocol allow a host to inform its local router, using Host Membership Reports, that it wants to receive messages addressed to a specific multicast group. All hosts conforming to Level 2 of the IP Multicasting specification require IGMP.

IP. See “Internet Protocol” on page 260.

IP Multicasting. Sending out data to distributed servers on the MBone (Multicast Backbone). For large amounts of data, IP Multicast is more efficient than normal Internet
transmissions because the server can broadcast a message to many recipients simultaneously. Unlike traditional Internet traffic that requires separate connections for each source-destination pair, IP Multicasting allows many recipients to share the same source. This means that just one set of packets is transmitted for all the destinations.

**Internet Protocol.** The method or protocol by which data is sent from one computer to another on the Internet. Each computer (known as a host) on the Internet has at least one IP address that uniquely identifies it among all other computers on the Internet. When you send or receive data (for example, an e-mail note or a Web page), the message gets divided into little chunks called packets. Each of these packets contains both the sender's Internet address and the receiver's address. Any packet is sent first to a gateway computer that understands a small part of the Internet. The gateway computer reads the destination address and forwards the packet to an adjacent gateway that in turn reads the destination address and so forth across the Internet until one gateway recognizes the packet as belonging to a computer within its immediate neighborhood or domain. That gateway then forwards the packet directly to the computer whose address is specified.

Because a message is divided into a number of packets, each packet can, if necessary, be sent by a different route across the Internet. Packets can arrive in a different order than they were sent. The Internet Protocol just delivers them. It's up to another protocol, the Transmission Control Protocol (TCP) to put them back in the right order. IP is a connectionless protocol, which means that there is no continuing connection between the end points that are communicating. Each packet that travels through the Internet is treated as an independent unit of data without any relation to any other unit of data. (The reason the packets do get put in the right order is because of TCP, the connection-oriented protocol that keeps track of the packet sequence in a message.) In the Open Systems Interconnection (OSI) communication model, IP is in Layer 3, the Networking Layer. The most widely used version of IP today is IP version 4 (IPv4). However, IP version 6 (IPv6) is also beginning to be supported. IPv6 provides for much longer addresses and therefore for the possibility of many more Internet users. IPv6 includes the capabilities of IPv4 and any server that can support IPv6 packets can also support IPv4 packets.

**J**

**Joint Test Action Group.** An IEEE group that specifies test framework
standards for electronic logic components.

**L**

**LAN.** See “Local Area Network” on page 261.

**Learning.** The bridge examines the Layer 2 source addresses of every frame on the attached networks (called listening) and then maintains a table, or cache, of which MAC addresses are attached to each of its ports.

**Link Aggregation.** IEEE 802.1AX-2008. A method using multiple network cables/ports in parallel to increase the link speed and the redundancy for higher availability (Load Balancing, Trunking).

**Link-State.** In routing protocols, the declared information about the available interfaces and available neighbors of a router or network. The protocol's topological database is formed from the collected link-state declarations.

**LLDP.** The IEEE 802.1AB standard for link layer discovery in Ethernet networks provides a method for switches, routers and access points to advertise their identification, configuration and capabilities to neighboring devices that store the data in a MIB (management information base). Link layer discovery allows a network management system to model the topology of the network by interrogating the MIB databases in the devices.

**Local Area Network.** A group of computers that are located in one area and are connected by less than 1,000 feet of cable. A typical LAN might interconnect computers and peripherals on a single floor or in a single building. LANs can be connected together, but if modems and telephones connect two or more LANs, the larger network constitutes what is called a WAN or Wide Area Network.

**M**

**MAC.** (1) Medium Access Control. In LANs, the sublayer of the data link control layer that supports medium-dependent functions and uses the services of the physical layer to provide services to the logical link control (LLC) sublayer. The MAC sublayer includes the method of determining when a device has access to the transmission medium. (2) Message Authentication Code. In computer security, a value that is a part of a message or accompanies a message and is used to determine that the contents, origin, author, or other attributes of all or part of the message are as they appear to be. *(IBM Glossary of Computing Terms)*

**Management Information Base.**

When SNMP devices send SNMP messages to the management
console (the device managing SNMP messages), it stores information in the MIB.

**MBONE.** See “Multicast Backbone” on page 262.

**MDC.** Management Data Clock.

**MDI.** Management Data Interface.

**MDIO.** Management Data Input/Output.

**MDIX.** Management Dependent Interface Crossover.

**MIB.** See “Management Information Base” on page 261.

**MOSPF.** See “Multicast OSPF” on page 262.

**MPLS.** See “Multi-Protocol Label Switching” on page 263.

**Multicast Backbone.** The MBONE is a virtual network. It is layered on top of portions of the physical Internet to support routing of IP multicast packets since that function has not yet been integrated into many production routers. The network is composed of islands that can directly support IP multicast, such as multicast LANs like Ethernet, linked by virtual point-to-point links called "tunnels". The tunnel endpoints are typically workstation-class machines having operating system support for IP multicast and running the "mrouted" multicast routing daemon.

**Multicasting.** To transmit a message to specific recipients across a network. A simple example of multicasting is sending an e-mail message to a mailing list. Teleconferencing and videoconferencing also use multicasting, but require more robust protocols and networks. Standards are being developed to support multicasting over a TCP/IP network such as the Internet. These standards, IP Multicast and Mbone, will allow users to easily join multicast groups. Note that multicasting refers to sending a message to a select group whereas broadcasting refers to sending a message to everyone connected to a network. The terms multicast and narrowcast are often used interchangeably, although narrowcast usually refers to the business model whereas multicast refers to the actual technology used to transmit the data.

**Multicast OSPF.** With a MOSPF specification, an IP Multicast packet is routed based both on the packet's source and its multicast destination (commonly referred to as source/destination routing). As it is routed, the multicast packet follows a shortest path to each multicast destination. During packet forwarding, any commonality of paths is exploited; when multiple hosts belong to a single multicast group, a multicast packet will be replicated only when the paths to the
separate hosts diverge. See “P” on page 263 for more information.

**Multiplexing.** A function within a layer that interleaves the information from multiple connections into one connection.

**Multi-Protocol Label Switching.**

An initiative that integrates Layer 2 information about network links (bandwidth, latency, utilization) into Layer 3 (IP) within a particular autonomous system—or ISP—in order to simplify and improve IP-packet exchange. MPLS gives network operators a great deal of flexibility to divert and route traffic around link failures, congestion, and bottlenecks. From a QoS standpoint, ISPs will better be able to manage different kinds of data streams based on priority and service plan. For instance, those who subscribe to a premium service plan, or those who receive a lot of streaming media or high-bandwidth content can see minimal latency and packet loss. When packets enter into a MPLS-based network, Label Edge Routers (LERs) give them a label (identifier). These labels not only contain information based on the routing table entry (i.e., destination, bandwidth, delay, and other metrics), but also refer to the IP header field (source IP address), Layer 4 socket number information, and differentiated service. Once this classification is complete and mapped, different packets are assigned to corresponding Labeled Switch Paths (LSPs), where Label Switch Routers (LSRs) place outgoing labels on the packets. With these LSPs, network operators can divert and route traffic based on data-stream type and Internet-access customer.

**MT-RJ connector.** A type of fiber-optic cable jack that is similar in shape and concept to a standard telephone jack, enabling duplex fiber-optic cables to be plugged into compatible devices as easily as plugging in a telephone cable.

**MUX.** See “Multiplexing” on page 263.

**O**

**Open Systems Interconnection.**

OSI is a seven (7) layer architecture model for communications systems developed by the ISO for the interconnection of data communications systems. Each layer uses and builds on the services provided by those below it.

**OS.** Operating System.

**OSI.** See “Open Systems Interconnection” on page 263.

**P**

**PDU.** See “Protocol Data Unit” on page 264.
**PHY.** The OSI Physical Layer: The physical layer provides for transmission of cells over a physical medium connecting two ATM devices. This physical layer is comprised of two sublayers: the Physical Medium Dependent (PMD) sublayer, and the Transmission Convergence (TC) sublayer.

**Port Mirroring.** Also known as a roving analysis port. This is a method of monitoring network traffic that forwards a copy of each incoming and outgoing packet from one port of a network switch to another port where the packet can be studied. A network administrator uses port mirroring as a diagnostic tool or debugging feature, especially when fending off an attack. It enables the administrator to keep close track of switch performance and alter it if necessary. Port mirroring can be managed locally or remotely. An administrator configures port mirroring by assigning a port from which to copy all packets and another port where those packets will be sent. A packet bound for or heading away from the first port will be forwarded onto the second port as well. The administrator places a protocol analyzer on the port receiving the mirrored data to monitor each segment separately. The analyzer captures and evaluates the data without affecting the client on the original port. The monitor port may be a port on the same SwitchModule with an attached RMON probe, a port on a different SwitchModule in the same hub, or the SwitchModule processor. Port mirroring can consume significant CPU resources while active. Better choices for long-term monitoring may include a passive tap like an optical probe or an Ethernet repeater.

**Protocol Data Unit.** PDU is a packet of data passed across a network. The term implies a specific layer of the OSI model and a specific protocol.

**Q**

**QoS.** See “Quality of Service” on page 264.

**Quality of Service.** QoS is a networking term that specifies a guaranteed level of throughput. Throughput is the amount of data transferred from one device to another or processed in a specified amount of time - typically, throughputs are measured in bytes per second (Bps).

**R**

**RFC.** Request For Comment.

**RMON.** Short for remote monitoring, a network management protocol that allows network information to be gathered at a single workstation. Whereas SNMP gathers network data from a single type of Management Information...
Base (MIB), RMON 1 defines nine additional MIBs that provide a much richer set of data about network usage. For RMON to work, network devices, such as hubs and switches, must be designed to support it. The newest version of RMON, RMON 2, provides data about traffic at the network layer in addition to the physical layer. This allows administrators to analyze traffic by protocol.

**RP.** Rendezvous Point. Used with IP Multicast.

**S**

**SDL.** Synchronous Data Link.

**Simple Network Management Protocol.** SNMP is the protocol governing network management and the monitoring of network devices and their functions. It is not necessarily limited to TCP/IP networks. The versions have the following differences:

- **SNMPv1** (full): Security is based on community strings.

- **SNMPsec** (historic): Security is based on parties. Few, if any, vendors implemented this version of the protocol, which is now largely forgotten.

- **SNMPv2p** (historic): For this version, much work was done to update the SNMPv1 protocol and the SMIv1, and not just security. The result was updated protocol operations, new protocol operations and data types, and party-based security from SNMPsec.

- **SNMPv2c** (experimental): This version of the protocol is called community string-based SNMPv2. It is an update of the protocol operations and data types of SNMPv2p, and uses community-based security from SNMPv1.

- **SNMPv2u** (experimental): This version of the protocol uses the protocol operations and data types of SNMPv2c and security based on users.

- **SNMPv2*** (experimental): This version combined the best features of SNMPv2p and SNMPv2u. (It is also called SNMPv2star.) The documents defining this version were never published as RFCs.

- **SNMPv3** (proposed): This version of the protocol is a combination of user-based security and the protocol operations and data types from SNMPv2p and support for proxies. The security is based on that found in SNMPv2u and SNMPv2*, and updated after much review. The documents defining this protocol will soon be published as RFCs.

**SimpleX signaling.** SX is one of IEEE 802.3’s designations for media. For example, 1000SX indicates 1000 gigabit Ethernet over "short haul" or "short wavelength" optical fiber.
SMII. Serial Media Independent Interface.

SNMP. See “Simple Network Management Protocol” on page 265.

SRAM. Static Random Access Memory.

STP. Spanning Tree Protocol. See “802.1D” on page 255 for more information.

Telnet. A character-based UNIX application that enables users with a Telnet server account to log on to a UNIX computer and utilize its resources.

TFTP. See “Trivial File Transfer Protocol” on page 266.

Trivial File Transfer Protocol.

TFTP is a simple form of the File Transfer Protocol (FTP). TFTP uses the User Datagram Protocol (UDP, a direct protocol used to communicate datagrams over a network with little error recovery) and provides no security features. It is often used by servers to boot diskless workstations, X-terminals, and routers.

Trunking. The process of combing a set of trunks that are traffic-engineered as a unit for the establishment of connections between switching systems in which all of the communications paths are interchangeable. See “Link Aggregation” on page 261.

V

Virtual Local Area Network.

Operating at the Data Link Layer (Layer 2 of the OSI model), the VLAN is a means of parsing a single network into logical user groups or organizations, as if they physically resided on a dedicated LAN segment of their own. In reality, this virtually defined community may have individual members peppered across a large, extended LAN. The VLAN identifier is part of the 802.1Q tag, which is added to an Ethernet frame by an 802.1Q-compliant switch or router. Devices recognizing 802.1Q-tagged frames maintain appropriate tables to track VLANs. The first three bits of the 802.1Q tag are used by 802.1P to establish priority for the packet.

VLAN. See “Virtual Local Area Network” on page 266.

vMAN. Virtual Metropolitan Area Network.

W

WAN. See “Wide Area Network” on page 267.

Web. Also known as World-Wide Web (WWW) or W3. An Internet client-server system to distribute
information, based upon the hypertext transfer protocol (HTTP).

**Wide Area Network.** A WAN is a computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more local-area networks (LANs).

X

**XModem.** One of the most popular file transfer protocols (FTPs). Xmodem is fairly effective at detecting errors. It sends blocks of data together with a checksum and then waits for acknowledgment of the block's receipt. The waiting slows down the rate of data transmission considerably, but it ensures accurate transmission. Xmodem can be implemented either in software or in hardware. Many modems, and almost all communications software packages, support Xmodem. However, it is useful only at relatively slow data transmission speeds (less than 4,800 bps). Enhanced versions of Xmodem that work at higher transmission speeds are known as Ymodem and Zmodem.
Index

7 Index

A
areaid 22
authentication login 247
auto-negotiate 95
auto-negotiate all 97

B
bridge aging-time 63
bridge fast-link-detection 64

C
classofservice dot1pmapping 57
classofservice ip-dscp-mapping 58
classofservice trust 59
clear arp-table-switch 146
clear commands
  clear arp-table-switch 146
  clear config 147
  clear pass 149
  clear traplog 150, 151
  clear config 147
  clear counters 147, 148
  clear eventlog 145
  clear igmp-snooping 148
  clear mac-addr-table 149
  clear pass 149
  clear signal-contacts 150
  Competence Center 273
config commands
  config port admin-mode 128, 129
  config port linktrap 130, 131
  config port physical-mode 133
  config users add 139, 140
  config users delete 138, 139, 140
  config users passwd 141
  config users delete 138, 139, 140, 141
  config users passwd 138, 139, 140, 141
  configuration reset 147
  copy 152

D
device configuration commands 201
device-status 154
dhcp-relay 242, 243
duplex settings 133

F
fast-hiper-ring 241

G
Global Config Mode 29

H
hiper-ring 237
hiper-ring mode 238
hiper-ring port primary 238
hiper-ring port secondary 239
hiper-ring recovery-delay 239

I
Interface Config Mode 30
inventory 118, 120, 121, 123, 124, 247
ip http server 253
ip http secure-server 253
ipaddr 21

L
Line Config Mode 30
link traps
  interface 130, 131
lldp 168
LLDP - Link Layer Discovery Protocol 161
lldp admin-state 173
lldp chassis tx-interval 172
lldp chassis tx-interval all 172
lldp config chassis admin-state 169
lldp config chassis notification-interval 170
lldp config chassis re-init-delay 170
lldp config chassis tx-delay 171
lldp config chassis tx-hold-mult 171
lldp fdb-mode 173
lldp hm-mode 174
lldp max-neighbors 174
lldp notification 175
lldp tlv 175, 176, 177, 178, 179
lldp tlv link-aggregation 175
lldp tlv mac-phy-config-state 175
lldp tlv max-frame-size 176
lldp tlv mgmt-addr 176
lldp tlv port-desc 176
lldp tlv protocol 177
lldp tlv sys-cap 178
lldp tlv sys-desc 179
lldp tlv sys-name 179
logging buffered 91
logging buffered wrap 92
logging cli-command 93
logging console 94
logical slot/port 22
## Index

| Logout | 155 |
| Logout command | 155 |

### M

| Maddr | 22 |
| Monitor session | 101 |
| Monitor session mode | 102, 103 |
| Mrp current-domain | 231 |
| Mrp delete-domain | 232 |
| Mrp new-domain | 233 |

### N

| Network javamode | 64 |
| Network parms | 65 |
| Network priority | 66 |
| Network protocol | 65 |
| Nmp | 131 |
| No dhcprelay | 242 |
| No lldp | 169 |
| No sntp | 186 |
| No sntp anycast address | 186, 187, 192 |
| No sntp client server | 189 |
| No sntp client server primary | 190, 191 |

### P

| Passwords |
| Changing user | 141 |
| Resetting all | 149 |

| Pong | 156 |
| Pong command | 154, 156, 157 |
| Poe - Power over Ethernet | 197 |

| Ports |
| Administrative mode | 128, 129 |
| Information | 126 |
| Link traps | 130, 131 |
| Physical mode | 133 |

| Privileged Exec Mode | 29 |
| PtP clock-mode | 195 |
| PtP operation | 196 |

### R

| Reboot | 159 |
| Reload | 159 |
| Reset system command | 159 |

### S

| Schulungsangebot | 273 |
| Selftest ramtest | 117 |
| Selftest reboot-on-error | 117 |
| Serial timeout | 67 |
| Sessions |
| Closing | 155 |
| Displaying | 135 |

| Set igmp | 104, 105, 109 |
| Set igmp aging-time-unknown | 106 |
| Set igmp automatic-mode | 106 |
| Set igmp forward-all | 107, 108 |
| Set igmp groupmembershipinterval | 110 |
| Set igmp interfacemode all | 111 |
| Set igmp lookup-interval-unknown | 112 |
| Set igmp lookup-resp-time-unknown | 112 |
| Set igmp maxresponse | 113 |
| Set igmp querier protocol-version | 114 |
| Set igmp querier tx-interval | 115 |
| Set igmp query-ports-to-filter | 116 |

| Set prompt | 68 |
| Show arp switch | 36 |
| Show authentication | 249 |
| Show authentication users | 250 |
| Show bridge aging-time | 36 |
| Show bridge fast-link-detection | 37 |
| Show bridge vlan-learning | 37 |
| Show classofservice dot1pmapping | 60 |
| Show classofservice ip-dscp-mapping | 61 |
| Show classofservice trust | 62 |

| Show commands |
| Show inventory | 118, 120, 121, 123, 124, 247 |
| Show loginsession | 135 |
| Show port | 126 |
| Show stats switch detailed | 40, 42, 47 |
| Show switchconfig | 127 |
| Show users | 136 |
| Show device-status | 38 |
| Show dhcprelay | 241 |
| Show eventlog | 39 |
| Show fast-hiper-ring | 241 |
| Show hiper-ring | 236 |
| Show hiper-ring info | 237 |
| Show igmpssnooping | 118 |
| Show interface | 40 |
| Show interface ethernet | 42 |
| Show interface switchport | 49 |
| Show lldp | 161 |
| Show lldp chassis tx-interval | 164 |
| Show lldp config | 161 |
| Show lldp config chassis | 162 |
| Show lldp config chassis admin-state | 162 |
| Show lldp config chassis notification-interval | 163 |

<p>| Show lldp config chassis re-init-delay | 163 |
| Show lldp config chassis tx-delay | 164 |
| Show lldp config chassis tx-hold-mult | 164 |
| Show lldp config port | 165 |
| Show lldp config port tlv | 166 |
| Show lldp remote-data | 167 |</p>
<table>
<thead>
<tr>
<th>Command/Parameter</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>show logging</td>
<td>49</td>
</tr>
<tr>
<td>show loginsession</td>
<td>135, 142, 143</td>
</tr>
<tr>
<td>show mac-addr-table</td>
<td>50</td>
</tr>
<tr>
<td>show mac-filter-table igmp-snooping</td>
<td>120</td>
</tr>
<tr>
<td>show mac-filter-table stats</td>
<td>124</td>
</tr>
<tr>
<td>show monitor</td>
<td>125</td>
</tr>
<tr>
<td>show mrp</td>
<td>229</td>
</tr>
<tr>
<td>show mrp current domain</td>
<td>230</td>
</tr>
<tr>
<td>show network</td>
<td>68</td>
</tr>
<tr>
<td>show port</td>
<td>126</td>
</tr>
<tr>
<td>show ptp</td>
<td>195</td>
</tr>
<tr>
<td>show running-config</td>
<td>53</td>
</tr>
<tr>
<td>show serial</td>
<td>70</td>
</tr>
<tr>
<td>show signal-contact</td>
<td>51</td>
</tr>
<tr>
<td>show slot</td>
<td>52</td>
</tr>
<tr>
<td>show snmp-access</td>
<td>70</td>
</tr>
<tr>
<td>show snmp-community</td>
<td>71</td>
</tr>
<tr>
<td>show snmptrap</td>
<td>72</td>
</tr>
<tr>
<td>show snmp</td>
<td>181</td>
</tr>
<tr>
<td>show snmp anycast</td>
<td>182</td>
</tr>
<tr>
<td>show snmp client</td>
<td>183</td>
</tr>
<tr>
<td>show snmp operation</td>
<td>184</td>
</tr>
<tr>
<td>show snmp server</td>
<td>184</td>
</tr>
<tr>
<td>show snmp status</td>
<td>185</td>
</tr>
<tr>
<td>show snmp time</td>
<td>185</td>
</tr>
<tr>
<td>show spanning-tree</td>
<td>201</td>
</tr>
<tr>
<td>show spanning-tree interface</td>
<td>203</td>
</tr>
<tr>
<td>show spanning-tree mst detailed</td>
<td>204</td>
</tr>
<tr>
<td>show spanning-tree mst port detailed</td>
<td>206</td>
</tr>
<tr>
<td>show sysinfo</td>
<td>53</td>
</tr>
<tr>
<td>show trapflags</td>
<td>73</td>
</tr>
<tr>
<td>show users</td>
<td>136</td>
</tr>
<tr>
<td>show users authentication</td>
<td>251</td>
</tr>
<tr>
<td>shutdown</td>
<td>128</td>
</tr>
<tr>
<td>shutdown all</td>
<td>129</td>
</tr>
<tr>
<td>signal-contact</td>
<td>156, 157</td>
</tr>
<tr>
<td>slot/port</td>
<td>22</td>
</tr>
<tr>
<td>snmp</td>
<td>130</td>
</tr>
<tr>
<td>snmp-access global</td>
<td>74</td>
</tr>
<tr>
<td>snmp-access version</td>
<td>75</td>
</tr>
<tr>
<td>snmp-server</td>
<td>76</td>
</tr>
<tr>
<td>snmp-server community</td>
<td>77</td>
</tr>
<tr>
<td>snmp-server community ipaddr</td>
<td>78</td>
</tr>
<tr>
<td>snmp-server community ipmask</td>
<td>79</td>
</tr>
<tr>
<td>snmp-server community mode</td>
<td>80</td>
</tr>
<tr>
<td>snmp-server community ro</td>
<td>81</td>
</tr>
<tr>
<td>snmp-server community rw</td>
<td>81</td>
</tr>
<tr>
<td>snmp-server enable traps</td>
<td>82</td>
</tr>
<tr>
<td>snmp-server enable traps stpmode</td>
<td>86</td>
</tr>
<tr>
<td>snmp-server location</td>
<td>81</td>
</tr>
<tr>
<td>snmp-server sysname</td>
<td>82</td>
</tr>
<tr>
<td>snmptrap</td>
<td>87</td>
</tr>
<tr>
<td>snmptrap ipaddr</td>
<td>88</td>
</tr>
<tr>
<td>snmptrap mode</td>
<td>89</td>
</tr>
<tr>
<td>snmptrap snmpversion</td>
<td>90</td>
</tr>
<tr>
<td>snmp trapflags</td>
<td>53</td>
</tr>
<tr>
<td>snmp user account management commands</td>
<td>135</td>
</tr>
<tr>
<td>snmp user account management commands 201 commands</td>
<td>135</td>
</tr>
<tr>
<td>System Utilities</td>
<td>145, 247</td>
</tr>
<tr>
<td>system utilities</td>
<td>145–156</td>
</tr>
<tr>
<td>T</td>
<td>146</td>
</tr>
<tr>
<td>U</td>
<td>135</td>
</tr>
<tr>
<td>VLAN Mode</td>
<td>29</td>
</tr>
</tbody>
</table>
Index

W
Web connections, displaying 135
Further support

- **Technical questions and training courses**
  In the event of technical queries, please contact your local Hirschmann distributor or Hirschmann office. You can find the addresses of our distributors on the Internet: www.hirschmann-ac.com

  Our support line is also at your disposal:
  - Phone +49 1805 14-1538
  - Fax +49 7127 14-1551

  Answers to Frequently Asked Questions can be found on the Hirschmann internet site (www.hirschmann-ac.com) at the end of the product sites in the FAQ category.
  The current training courses to technology and products can be found under www.hicomcenter.com.

- **Hirschmann Competence Center**
  In the long term, excellent products alone do not guarantee a successful customer relationship. Only comprehensive service makes a difference worldwide. In the current global competition scenario, the Hirschmann Competence Center is ahead of its competitors on three counts with its complete range of innovative services:

  - Consulting incorporates comprehensive technical advice, from system evaluation through network planning to project planning.
  - Training offers you an introduction to the basics, product briefing and user training with certification.
  - Support ranges from the first installation through the standby service to maintenance concepts.

  With the Hirschmann Competence Center, you decided against making any compromises. Our client-customized package leaves you free to choose the service components that you want to use.
  Internet: www.hicomcenter.com