Command Line Interface Reference Guide
HP BladeSystem PC Blade Switch

Document Part Number: 413354-001

December 2005
WARNING: Text set off in this manner indicates that failure to follow directions could result in bodily harm or loss of life.

CAUTION: Text set off in this manner indicates that failure to follow directions could result in damage to equipment or loss of information.

CLI Reference Guide
HP BladeSystem PC Blade Switch

First Edition (December 2005)
Document Part Number: 413354-001
Contents

Command Line Interface
   Using the Command Line Interface (CLI) ........................................ 1–1
   Entering Commands .................................................................... 1–3
   Command Groups ....................................................................... 1–7

802.1x Commands
   aaa authentication dot1x ............................................................ 2–1
   dot1x system-auth-control ....................................................... 2–2
   dot1x port-control ................................................................. 2–3
   dot1x re-authentication .......................................................... 2–4
   dot1x timeout re-authperiod ................................................... 2–5
   dot1x re-authenticate .............................................................. 2–6
   dot1x timeout quiet-period ..................................................... 2–7
   dot1x timeout tx-period .......................................................... 2–8
   dot1x max-req ........................................................................ 2–9
   dot1x timeout supp-timeout ...................................................... 2–10
   dot1x timeout server-timeout .................................................. 2–11
   show dot1x .......................................................................... 2–12
   show dot1x users .................................................................... 2–15
   show dot1x statistics ............................................................... 2–16
   Advanced Features .................................................................. 2–18
   dot1x auth-not-req ................................................................... 2–18
   dot1x multiple-hosts ............................................................... 2–19
   dot1x single-host-violation ...................................................... 2–20
   dot1x guest-vlan ................................................................. 2–21
   dot1x guest-vlan enable .......................................................... 2–22
   show dot1x advanced .............................................................. 2–23

AAA Commands
   aaa authentication login .......................................................... 3–1
   aaa authentication enable ....................................................... 3–3
   login authentication ............................................................... 3–5
   enable authentication ............................................................ 3–6
   ip http authentication ............................................................. 3–7
   ip https authentication .......................................................... 3–8
   show authentication methods ............................................... 3–9
   password .............................................................................. 3–10
   enable password ................................................................. 3–11
   username ............................................................................. 3–12
Contents

ACL Commands

ip access-list .................................................. 4–1
permit (IP) ..................................................... 4–2
deny (IP) ....................................................... 4–5
mac access-list ................................................. 4–7
permit (MAC) ................................................... 4–8
deny (MAC) ..................................................... 4–9
service-acl ....................................................... 4–11
show access-lists ................................................. 4–12

Address Table Commands

bridge address ..................................................... 5–1
bridge multicast filtering ....................................... 5–3
bridge multicast address ....................................... 5–4
bridge multicast forbidden address ......................... 5–5
bridge multicast forward-all ................................ 5–6
bridge multicast forbidden forward-all ..................... 5–7
bridge aging-time ............................................... 5–8
clear bridge ...................................................... 5–9
port security ..................................................... 5–10
port security mode ............................................. 5–11
port security max ............................................... 5–12
port security routed secure-address ....................... 5–13
show bridge address-table ................................... 5–14
show bridge address-table static ........................... 5–15
show bridge address-table count ............................ 5–16
show bridge multicast address-table ....................... 5–17
show bridge multicast filtering ............................... 5–19
show ports security ............................................. 5–20
show ports security addresses ............................... 5–21
Clock Commands

- clock set ......................................................... 6–1
- clock source ....................................................... 6–2
- clock timezone ..................................................... 6–3
- clock summer-time ............................................. 6–4
- snntp authentication-key .......................................... 6–6
- snntp authenticate ................................................ 6–7
- snntp trusted-key ................................................ 6–8
- snntp client poll timer ......................................... 6–9
- snntp broadcast client enable .................................. 6–10
- snntp anycast client enable ..................................... 6–11
- snntp client enable (Interface) ................................ 6–12
- snntp unicast client enable ...................................... 6–13
- snntp unicast client poll ....................................... 6–14
- snntp server ......................................................... 6–15
- show clock .......................................................... 6–16
- show snntp configuration ......................................... 6–17
- show snntp status .................................................. 6–18

Configuration and Image File Commands

- copy ................................................................. 7–1
- delete ................................................................. 7–4
- boot system ......................................................... 7–5
- show running-config ............................................... 7–6
- show startup-config ............................................. 7–7
- show bootvar ....................................................... 7–8
Ethernet Configuration Commands

interface ethernet .......................................................... 8–1
description ................................................................. 8–4
speed ................................................................. 8–5
duplex ................................................................. 8–6
negotiation ......................................................... 8–7
flowcontrol .......................................................... 8–8
mdix ................................................................. 8–9
back-pressure .......................................................... 8–10
clear counters .......................................................... 8–11
set interface active ...................................................... 8–12
show interfaces advertise ................................................... 8–13
show interfaces configuration .......................................... 8–14
show interfaces status ...................................................... 8–15
show interfaces description ............................................. 8–16
show interfaces counters .................................................. 8–17
port storm-control include-multicast (IC) . . . . . . . . . . . . . . . . . 8–20
port storm-control broadcast enable .................................. 8–21
port storm-control broadcast rate ...................................... 8–22
show ports storm-control .................................................. 8–23

GVRP Commands

gvrp enable (Global) ..................................................... 9–1
gvrp enable (Interface) .................................................... 9–2
garp timer ................................................................. 9–3
gvrp vlan-creation-forbid ................................................. 9–4
gvrp registration-forbid .................................................. 9–5
clear gvrp statistics .......................................................... 9–6
show gvrp configuration .................................................... 9–7
show gvrp statistics .......................................................... 9–8
show gvrp error-statistics .................................................. 9–9

IGMP Snooping Commands

ip igmp snooping (Global). .................................................. 10–1
ip igmp snooping (Interface) ................................................. 10–2
nip igmp snooping host-time-out ........................................ 10–3
ip igmp snooping mrouter-time-out ....................................... 10–4
ip igmp snooping mrouter learn-pim-dvmrp ................................ 10–5
ip igmp snooping leave-time-out ........................................... 10–6
show ip igmp snooping mrouter ............................................. 10–7
show ip igmp snooping interface ......................................... 10–8
show ip igmp snooping groups ............................................... 10–9
IP Addressing Commands

- ip address ........................................... 11–1
- ip address dhcp ..................................... 11–2
- ip default-gateway .................................. 11–3
- show ip interface .................................... 11–4
- arp ...................................................... 11–5
- arp timeout .......................................... 11–6
- clear arp-cache ..................................... 11–7
- show arp ............................................. 11–8
- ip domain-lookup ................................. 11–9
- ip domain-name .................................... 11–10
- ip name-server ...................................... 11–11
- ip host ............................................... 11–12
- clear host .......................................... 11–13
- clear host dhcp ..................................... 11–14
- show hosts ......................................... 11–15

LACP Commands

- lacp system-priority ................................ 12–1
- lacp port-priority .................................. 12–2
- lacp timeout ........................................ 12–3
- show lacp ethernet .................................. 12–4
- show lacp port-channel ............................ 12–6

Line Commands

- line .................................................... 13–1
- speed .................................................. 13–2
- autobaud ............................................ 13–3
- exec-timeout ....................................... 13–4
- history .............................................. 13–5
- history size ........................................ 13–6
- terminal history ................................... 13–7
- terminal history size .............................. 13–8
- show line .......................................... 13–9

Management ACL Commands

- management access-list .......................... 14–1
- permit (Management) .............................. 14–3
- deny (Management) ............................... 14–4
- management access-class ...................... 14–5
- show management access-list ................. 14–6
- show management access-class ............... 14–7
Contents

PHY Diagnostics Commands

test copper-port tdr ........................................ 15–1
show copper-ports tdr .................................... 15–2
show copper-ports cable-length ......................... 15–3
show fiber-ports optical-transceiver .................... 15–4

Port Channel Commands

interface port-channel ...................................... 16–1
interface range port-channel ............................... 16–2
channel-group ............................................... 16–3
show interfaces port-channel ............................... 16–4

Port Monitor Commands

port monitor .................................................... 17–1
show ports monitor .......................................... 17–3

QoS Commands

qos .......................................................... 18–1
show qos ...................................................... 18–2
class-map ..................................................... 18–3
show class-map .............................................. 18–5
match .......................................................... 18–6
policy-map .................................................... 18–7
class .......................................................... 18–8
show policy-map ............................................ 18–9
trust cos-dscp ............................................ 18–10
set ............................................................ 18–11
police .......................................................... 18–12
service-policy ............................................... 18–13
qos aggregate-policer ..................................... 18–14
show qos aggregate-policer ............................... 18–15
police aggregate ............................................ 18–16
wrr-queue cos-map ........................................ 18–17
priority-queue out num-of-queues ....................... 18–18
traffic-shape .................................................. 18–19
show qos interface .......................................... 18–20
wrr-queue threshold ....................................... 18–22
qos map dscp-dp ........................................... 18–23
qos map policed-dscp .................................... 18–24
qos map dscp-queue ....................................... 18–25
qos trust (Global) .......................................... 18–26
qos cos ....................................................... 18–28
qos dscp-mutation ......................................... 18–29
qos map dscp-mutation .................................... 18–30
RADIUS Commands

radius-server host ................................................................. 19–1
radius-server key ................................................................. 19–3
radius-server retransmit ........................................................ 19–4
radius-server source-ip ......................................................... 19–5
radius-server timeout ........................................................... 19–6
radius-server deadtime .......................................................... 19–7
show radius-servers .............................................................. 19–8

RMON Commands

show rmon statistics ............................................................. 20–1
rmon collection history ........................................................ 20–4
show rmon collection history .................................................. 20–5
show rmon history ............................................................... 20–6
rmon alarm .......................................................... 20–9
show rmon alarm-table .......................................................... 20–11
show rmon alarm ............................................................... 20–12
rmon event .......................................................... 20–14
show rmon events .............................................................. 20–15
show rmon log ................................................................. 20–16
rmon table-size ................................................................. 20–17

SNMP Commands

snmp-server community .......................................................... 21–1
snmp-server view ................................................................. 21–3
snmp-server group ............................................................... 21–4
snmp-server user ................................................................. 21–5
snmp-server engineid local ...................................................... 21–7
snmp-server enable traps ......................................................... 21–9
snmp-server filter ................................................................. 21–10
snmp-server host ................................................................. 21–11
snmp-server v3-host ............................................................. 21–13
snmp-server trap authentication ................................................ 21–14
snmp-server contact ............................................................. 21–15
snmp-server location ............................................................. 21–16
snmp-server set ................................................................. 21–17
show snmp ................................................................. 21–18
show snmp engineid ............................................................. 21–20
show snmp views ................................................................. 21–21
show snmp groups ............................................................... 21–22
show snmp filters ................................................................. 21–23
show snmp users ................................................................. 21–24
Spanning-Tree Commands

spanning-tree .................................................. 22–1
spanning-tree mode .............................................. 22–2
spanning-tree forward-time .................................... 22–3
spanning-tree hello-time ....................................... 22–4
spanning-tree max-age ......................................... 22–5
spanning-tree priority .......................................... 22–6
spanning-tree disable .......................................... 22–7
spanning-tree cost .............................................. 22–8
spanning-tree port-priority .................................... 22–9
spanning-tree portfast .......................................... 22–10
spanning-tree link-type ........................................ 22–11
spanning-tree pathcost method ................................ 22–12
spanning-tree bpdu .............................................. 22–13
clear spanning-tree detected-protocols ...................... 22–14
spanning-tree mst priority .................................... 22–15
spanning-tree mst max-hops .................................. 22–16
spanning-tree mst port-priority ................................ 22–17
spanning-tree mst cost .......................................... 22–18
spanning-tree mst configuration .............................. 22–19
instance (mst) .................................................. 22–20
name (mst) ..................................................... 22–21
revision (mst) .................................................. 22–22
show (mst) ...................................................... 22–23
exit (mst) ...................................................... 22–24
abort (mst) ..................................................... 22–25
spanning-tree guard root ...................................... 22–26
show spanning-tree ............................................. 22–27
spanning-tree pvst-interop .................................. 22–39
spanning-tree mst mstp-rstp ................................ 22–40

SSH Commands

ip ssh port ...................................................... 23–1
ip ssh server .................................................... 23–2
crypto key generate dsa ........................................ 23–3
crypto key generate rsa ........................................ 23–4
ip ssh pubkey-auth ............................................ 23–5
crypto key pubkey-chain ssh ................................. 23–6
user-key ....................................................... 23–7
key-string ..................................................... 23–8
show ip ssh .................................................... 23–10
## Syslog Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>logging on</td>
<td>24–1</td>
</tr>
<tr>
<td>logging</td>
<td>24–2</td>
</tr>
<tr>
<td>logging console</td>
<td>24–3</td>
</tr>
<tr>
<td>logging buffered</td>
<td>24–4</td>
</tr>
<tr>
<td>logging buffered size</td>
<td>24–5</td>
</tr>
<tr>
<td>clear logging</td>
<td>24–6</td>
</tr>
<tr>
<td>logging file</td>
<td>24–7</td>
</tr>
<tr>
<td>clear logging file</td>
<td>24–8</td>
</tr>
<tr>
<td>aaa logging</td>
<td>24–9</td>
</tr>
<tr>
<td>file-system logging</td>
<td>24–10</td>
</tr>
<tr>
<td>management logging</td>
<td>24–11</td>
</tr>
<tr>
<td>show logging</td>
<td>24–12</td>
</tr>
<tr>
<td>show logging file</td>
<td>24–14</td>
</tr>
</tbody>
</table>

## System Management Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ping</td>
<td>25–1</td>
</tr>
<tr>
<td>traceroute</td>
<td>25–3</td>
</tr>
<tr>
<td>telnet</td>
<td>25–5</td>
</tr>
<tr>
<td>resume</td>
<td>25–8</td>
</tr>
<tr>
<td>reload</td>
<td>25–9</td>
</tr>
<tr>
<td>hostname</td>
<td>25–10</td>
</tr>
<tr>
<td>show users</td>
<td>25–11</td>
</tr>
<tr>
<td>show sessions</td>
<td>25–12</td>
</tr>
<tr>
<td>show system</td>
<td>25–13</td>
</tr>
<tr>
<td>show version</td>
<td>25–14</td>
</tr>
<tr>
<td>service cpu-utilization</td>
<td>25–15</td>
</tr>
<tr>
<td>show cpu utilization</td>
<td>25–16</td>
</tr>
</tbody>
</table>

## TACACS+ Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>tacacs-server host</td>
<td>26–1</td>
</tr>
<tr>
<td>tacacs-server key</td>
<td>26–3</td>
</tr>
<tr>
<td>tacacs-server timeout</td>
<td>26–4</td>
</tr>
<tr>
<td>tacacs-server source-ip</td>
<td>26–5</td>
</tr>
<tr>
<td>show tacacs</td>
<td>26–6</td>
</tr>
</tbody>
</table>
## User Interface Commands

- **do**: 27–1
- **enable**: 27–2
- **disable**: 27–3
- **login**: 27–4
- **configure**: 27–5
- **exit (Configuration)**: 27–6
- **exit**: 27–7
- **end**: 27–8
- **help**: 27–9
- **terminal data-dump**: 27–10
- **show history**: 27–11
- **show privilege**: 27–12

## VLAN Commands

- **vlan database**: 28–1
- **vlan**: 28–2
- **interface vlan**: 28–3
- **interface range vlan**: 28–4
- **name**: 28–5
- **switchport mode**: 28–6
- **switchport access vlan**: 28–7
- **switchport trunk allowed vlan**: 28–8
- **switchport trunk native vlan**: 28–9
- **switchport general allowed vlan**: 28–10
- **switchport general pvid**: 28–11
- **switchport general ingress-filtering disable**: 28–12
- **switchport general acceptable-frame-type tagged-only**: 28–13
- **switchport forbidden vlan**: 28–14
- **ip internal-usage-vlan**: 28–15
- **show vlan**: 28–16
- **show vlan internal usage**: 28–17
- **show interfaces switchport**: 28–18

## Web Server Commands

- **ip http server**: 29–1
- **ip http port**: 29–2
- **ip https server**: 29–3
- **ip https port**: 29–4
- **crypto certificate generate**: 29–5
- **crypto certificate request**: 29–7
- **crypto certificate import**: 29–9
- **ip https certificate**: 29–11
- **show crypto certificate mycertificate**: 29–12
- **show ip http**: 29–13
- **show ip https**: 29–14

## Index

- **ip https server**: 29–1
- **vlan**: 28–2
- **enable**: 27–2
- **login**: 27–4
- **configure**: 27–5
- **show history**: 27–11
- **show privilege**: 27–12
Using the Command Line Interface (CLI)

Accessing the CLI

When accessing the management interface for the switch over a direct connection to the server’s console port, or via a Telnet connection, the switch can be managed by entering command keywords and parameters at the prompt. Using the switch’s command-line interface (CLI) is very similar to entering commands on a UNIX system.

Console Connection

To access the switch through the console port, perform these steps:

1. At the console prompt, enter the user name and password. When the administrator user name and password is entered, the CLI displays the “Console#” prompt and enters privileged access mode (i.e., Privileged Exec). But when the guest user name and password is entered, the CLI displays the “Console>” prompt and enters normal access mode (i.e., Normal Exec).

2. Enter the necessary commands to complete your desired tasks.

3. When finished, exit the session with the “quit” or “exit” command.

After connecting to the system through the console port, the login screen displays:

User Access Verification
Username: admin
Password:

- CLI session with the PC Blade Switch is opened.
- To end the CLI session, enter [Exit].

Console#

Telnet Connection

Telnet operates over the IP transport protocol. In this environment, your management station and any network device you want to manage over the network must have a valid IP address. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. Each address consists of a network portion and host portion.

For example, the IP address assigned to this switch, 10.1.0.1, consists of a network portion (10.1.0) and a host portion (1).

✎ The IP address for this switch is unassigned by default.
To access the switch through a Telnet session, you must first set the IP address for the switch, and set the default gateway if you are managing the switch from a different IP subnet.

For example:

```
Console(config)#interface vlan 1
Console(config-if)#ip address 10.1.0.1 255.255.255.0
Console(config-if)#exit
Console(config)#ip default-gateway 10.1.0.254
```

If your corporate network is connected to another network outside your office or to the Internet, you need to apply for a registered IP address. However, if you are attached to an isolated network, then you can use any IP address that matches the network segment to which you are attached.

After you configure the switch with an IP address, you can open a Telnet session by performing these steps:

1. From the remote host, enter the Telnet command and the IP address of the device you want to access.
2. At the prompt, enter the user name and system password. The CLI will display the “Console#” prompt for the administrator to show that you are using privileged access mode (i.e., Privileged Exec), or “Console” for the guest to show that you are using normal access mode (i.e., Normal Exec).
3. Enter the necessary commands to complete your desired tasks.
4. When finished, exit the session with the “quit” or “exit” command.

After entering the Telnet command, the login screen displays:

```
Username: admin
Password:

   CLI session with the PC Blade Switch is opened.
   To end the CLI session, enter [Exit].

   Console#
```

You can open up to four sessions to the device via Telnet.
**Entering Commands**

This section describes how to enter CLI commands.

**Keywords and Arguments**

A CLI command is a series of keywords and arguments. Keywords identify a command, and arguments specify configuration parameters. For example, in the command “show interfaces status ethernet 1/e5,” `show interfaces` and `status` are keywords, `ethernet` is an argument that specifies the interface type, and `1/5` specifies the port.

You can enter commands as follows:

- To enter a simple command, enter the command keyword.
- To enter multiple commands, enter each command in the required order. For example, to enable Privileged Exec command mode, and display the startup configuration, enter:

  ```
  Console> enable
  Console# show startup-config
  ```

- To enter commands that require parameters, enter the required parameters after the command keyword. For example, to set a password for the administrator, enter:

  ```
  Console(config)# username admin password smith
  ```

**Minimum Abbreviation**

The CLI will accept a minimum number of characters that uniquely identify a command. For example, the command “configure” can be entered as `con`. If an entry is ambiguous, the system will prompt for further input.

**Command Completion**

If you terminate input with a Tab key, the CLI will print the remaining characters of a partial keyword up to the point of ambiguity. In the “logging history” example, typing `log` followed by a tab will result in printing the command up to “logging.”

**Getting Help on Commands**

You can display a brief description of the help system by entering the `help` command. You can also display command syntax by using the “?” character to list keywords or parameters.

**Show Commands**

If you enter a “?” at the command prompt, the system will display the first level of keywords for the current command class (Normal Exec or Privileged Exec) or configuration class (Global, ACL, DHCP, Interface, Line, VLAN Database, or MSTP). You can also display a list of valid keywords for a specific command. For example, the command “show ?” displays a list of possible show commands.
The command “show interfaces ?” will display the following information:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>counters</td>
<td>Information of interfaces counters</td>
</tr>
<tr>
<td>protocol-vlan</td>
<td>Protocol-vlan information</td>
</tr>
<tr>
<td>status s</td>
<td>Information of interfaces status</td>
</tr>
<tr>
<td>switchport</td>
<td>Information of interfaces switchport</td>
</tr>
</tbody>
</table>

**Partial Keyword Lookup**

If you terminate a partial keyword with a question mark, alternatives that match the initial letters are provided. (Remember not to leave a space between the command and question mark.) For example “s?” shows all the keywords starting with “s.”

**Negating the Effect of Commands**

For many configuration commands you can enter the prefix keyword “no” to cancel the effect of a command or reset the configuration to the default value. For example, the `logging` command will log system messages to a host server. To disable logging, specify the `no logging` command. This guide describes the negation effect for all applicable commands.

**Using Command History**

The CLI maintains a history of commands that have been entered. You can scroll back through the history of commands by pressing the up arrow key. Any command displayed in the history list can be executed again, or first modified and then executed.

Using the `show history` command displays a longer list of recently executed commands.

**Understanding Command Modes**

The command set is divided into Exec and Configuration classes. Exec commands generally display information on system status or clear statistical counters. Configuration commands, on the other hand, modify interface parameters or enable certain switching functions. These classes are further divided into different modes. Available commands depend on the selected mode. You can always enter a question mark “?” at the prompt to display a list of the commands available for the current mode.

**Exec Commands**

When you open a new console session on the switch with the user name and password “guest,” the system enters the Normal Exec command mode (or guest mode), displaying the “Console>” command prompt. Only a limited number of the commands are available in this mode. You can access all commands only from the Privileged Exec command mode (or administrator mode).
To access the Privilege Exec mode, open a new console session with the user name and password “admin.” The system will now display the “Console#” command prompt. You can also enter the Privileged Exec mode from within Normal Exec mode. To enter the Privileged Exec mode, enter the following user names and passwords:

<table>
<thead>
<tr>
<th>Username: admin</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password: [admin login password]</td>
</tr>
<tr>
<td>CLI session with the PC Blade Switch is opened.</td>
</tr>
<tr>
<td>To end the CLI session, enter [Exit].</td>
</tr>
<tr>
<td>Console#</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Username: guest</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password: [guest login password]</td>
</tr>
<tr>
<td>CLI session with the PC Blade Switch is opened.</td>
</tr>
<tr>
<td>To end the CLI session, enter [Exit].</td>
</tr>
<tr>
<td>Console# enable</td>
</tr>
<tr>
<td>Password: [privileged level password]</td>
</tr>
<tr>
<td>Console#</td>
</tr>
</tbody>
</table>

### Configuration Commands

Configuration commands are privileged level commands used to modify switch settings. These commands modify the running configuration only and are not saved when the switch is rebooted. To store the running configuration in non-volatile storage, use the `copy running-config startup-config` command.

The configuration commands are organized into different modes:

- **Global Configuration** — These commands modify the system level configuration, and include commands such as `hostname` and `snmp-server community`.
- **Access Control List Configuration** — These commands are used for packet filtering.
- **DHCP Configuration** — These commands are used to configure the DHCP server.
- **Interface Configuration** — These commands modify the port configuration such as `speed-duplex` and `negotiation`.
- **Line Configuration** — These commands modify the console port and Telnet configuration, and include command such as `parity` and `databits`.
- **Router Configuration** — These commands configure global settings for unicast and multicast routing protocols.
- **VLAN Configuration** — Includes the command to create VLAN groups.
- **Multiple Spanning Tree Configuration** — These commands configure settings for the selected multiple spanning tree instance.
To enter the Global Configuration mode, enter the command `configure` in Privileged Exec mode. The system prompt will change to “Console(config)#” which gives you access privilege to all Global Configuration commands.

```
Console# configure
Console(config)#
```

To enter the other modes, at the configuration prompt type one of the following commands. Use the exit or end command to return to the Privileged Exec mode. For example, you can use the following commands to enter interface configuration mode, and then return to Privileged Exec mode.

```
Console(config)# interface ethernet 1/e5
Console(config-if)# exit
Console(config)#
```

**Command Line Processing**

Commands are not case sensitive. You can abbreviate commands and parameters as long as they contain enough letters to differentiate them from any other currently available commands or parameters. You can use the Tab key to complete partial commands, or enter a partial command followed by the “?” character to display a list of possible matches. You can also use the following editing keystrokes for command-line processing:

### Keystroke Commands

<table>
<thead>
<tr>
<th>Keystroke</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up Arrows</td>
<td>Recalls commands from the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.</td>
</tr>
<tr>
<td>Down Arrows</td>
<td>Returns the most recent commands from the history buffer after recalling commands with the up arrow key. Repeating the key sequence will recall successively more recent commands.</td>
</tr>
<tr>
<td>Ctrl+A</td>
<td>Moves the cursor to the beginning of the command line.</td>
</tr>
<tr>
<td>Ctrl+E</td>
<td>Moves the cursor to the end of the command line.</td>
</tr>
<tr>
<td>Ctrl+Z/End</td>
<td>Returns back to the Privileged EXEC mode from any configuration mode.</td>
</tr>
</tbody>
</table>
## Command Groups

The system commands can be broken down into the functional groups shown below.

<table>
<thead>
<tr>
<th>Command Group</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1x Commands</td>
<td>Specify authentication, authorization and accounting (AAA) methods for use on interfaces running IEEE 802.1x, and enable 802.1x globally.</td>
<td>2-1</td>
</tr>
<tr>
<td>AAA Commands</td>
<td>Define the authentication method lists for servers.</td>
<td>3-1</td>
</tr>
<tr>
<td>ACL Commands</td>
<td>Display Access Control Lists (ACLs) defined on the device.</td>
<td>4-1</td>
</tr>
<tr>
<td>Address Table Commands</td>
<td>Register MAC-layer multicast addresses, and handle MAC-layer secure address to a routed port.</td>
<td>5-1</td>
</tr>
<tr>
<td>Clock Commands</td>
<td>Show the configuration or status of the Simple Network Time Protocol (SNTP).</td>
<td>6-1</td>
</tr>
<tr>
<td>Configuration and Image File Commands</td>
<td>Display the contents of the currently running configuration file, specify contents of image files.</td>
<td>7-1</td>
</tr>
<tr>
<td>Ethernet Configuration Commands</td>
<td>Configure multiple Ethernet type interfaces.</td>
<td>8-1</td>
</tr>
<tr>
<td>GVRP Commands</td>
<td>Display the GARP VLAN Registration Protocol (GVRP) configuration information, enable GVRP globally or on an interface.</td>
<td>9-1</td>
</tr>
<tr>
<td>IGMP Snooping Commands</td>
<td>Enable the Internet Group Management Protocol (IGMP) snooping.</td>
<td>10-1</td>
</tr>
<tr>
<td>IP Addressing Commands</td>
<td>Define a default gateway, set an IP address for interface, delete entries from the host.</td>
<td>11-1</td>
</tr>
<tr>
<td>LACP Commands</td>
<td>Configure system or port priority using the Link Aggregation Control Protocol (LACP).</td>
<td>12-1</td>
</tr>
<tr>
<td>Line Commands</td>
<td>Display line parameters, enable the command history function, or configure the command history buffer size.</td>
<td>13-1</td>
</tr>
<tr>
<td>Management ACL Commands</td>
<td>Define a permit or deny a rule, or configure a management access control list.</td>
<td>14-1</td>
</tr>
<tr>
<td>PHY Diagnostics Commands</td>
<td>Display the optical transceiver diagnostics.</td>
<td>15-1</td>
</tr>
<tr>
<td>Port Channel Commands</td>
<td>Enter the interface configuration mode to configure a specific, or a multiple port-channel.</td>
<td>16-1</td>
</tr>
<tr>
<td>Port Monitor Commands</td>
<td>Start a port monitoring session, or display the port monitoring status.</td>
<td>17-1</td>
</tr>
<tr>
<td>QoS Commands</td>
<td>Enable Quality of Service (QoS) on the device, create policy maps, and define traffic classifications</td>
<td>18-1</td>
</tr>
<tr>
<td>Command Group</td>
<td>Description</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>RADIUS Commands</td>
<td>Specify the source IP address used for communication with Remote Authentication Dial-in User Service (RADIUS) servers, and display the RADIUS server settings.</td>
<td>19-1</td>
</tr>
<tr>
<td>RMON Commands</td>
<td>Display the Remote Network Monitoring (RMON) Ethernet history statistics, alarms table and configuration.</td>
<td>20-1</td>
</tr>
<tr>
<td>SNMP Commands</td>
<td>Configure the community access string to permit access to the Simple Network Management Protocol (SNMP) server, create or update SNMP server entries, and specify SNMP engineID.</td>
<td>21-1</td>
</tr>
<tr>
<td>Spanning-Tree Commands</td>
<td>Configure the spanning-tree functionality.</td>
<td>22-1</td>
</tr>
<tr>
<td>SSH Commands</td>
<td>Display the Secure Socket Shell (SSH) public keys on the device, SSH server configuration, or which SSH public key is manually configured.</td>
<td>23-1</td>
</tr>
<tr>
<td>Syslog Commands</td>
<td>Log messages to a syslog server, or limit log messages to a syslog server.</td>
<td>24-1</td>
</tr>
<tr>
<td>System Management Commands</td>
<td>Display and list system, version or Telnet session information.</td>
<td>25-1</td>
</tr>
<tr>
<td>TACACS+ Commands</td>
<td>Display configuration and statistical information about a Terminal Access Controller Access Control System (TACACS+) server, or specify a TACACS+ host.</td>
<td>26-1</td>
</tr>
<tr>
<td>User Interface Commands</td>
<td>Display and list system, version or Telnet session information.</td>
<td>27-1</td>
</tr>
<tr>
<td>VLAN Commands</td>
<td>Enter the (Virtual Local Area Network) VLAN Configuration mode, enable simultaneously configuring multiple VLANs, or adds or remove VLANs.</td>
<td>28-1</td>
</tr>
<tr>
<td>Web Server Commands</td>
<td>Enable configuring the device from a browser, or display the HTTP server configuration.</td>
<td>29-1</td>
</tr>
</tbody>
</table>
aaa authentication dot1x

The **aaa authentication dot1x** Global Configuration mode command specifies one or more authentication, authorization, and accounting (AAA) methods for use on interfaces running IEEE 802.1x. To return to the default configuration, use the `no` form of this command.

**Syntax**

```plaintext
aaa authentication dot1x default method1 [method2...]
no aaa authentication dot1x default
```

**Parameters**

- `method1 [method2...]` - At least one keyword, as listed in the following table:

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>radius</td>
<td>Uses the list of all RADIUS servers for authentication.</td>
</tr>
<tr>
<td>none</td>
<td>Uses no authentication.</td>
</tr>
</tbody>
</table>

**Default Setting**

No authentication method is defined.

**Command Mode**

Global Configuration

**Command Usage**

Additional methods of authentication are used only if the previous method returns an error and not if the request for authentication is denied. To ensure that authentication succeeds even if all methods return an error, specify `none` as the final method in the command line.

The RADIUS server must support MD-5 challenge and EAP type frames.

**Example**

The following command uses the `aaa authentication dot1x default` with no authentication.

```plaintext
Console(config)# aaa authentication dot1x default none
```
**dot1x system-auth-control**

The `dot1x system-auth-control` Global Configuration mode command enables 802.1x globally. To return to the default configuration, use the `no` form of this command.

**Syntax**

dot1x system-auth-control  
no dot1x system-auth-control

**Parameters**

There are no parameters for this command.

**Default Configuration**

802.1x is disabled globally.

**Command Modes**

Global Configuration mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command enables 802.1x globally.

```
Console(config)# dot1x system-auth-control
```
dot1x port-control

The dot1x port-control Interface Configuration mode command enables manually controlling the authorization state of the port. To return to the default configuration, use the no form of this command.

Syntax

dot1x port-control {auto | force-authorized | force-unauthorized}

no dot1x port-control

Parameters

- **auto** — Enables 802.1x authentication on the interface and causes the port to transition to the authorized or unauthorized state based on the 802.1x authentication exchange between the port and the client.

- **force-authorized** — Disables 802.1x authentication on the interface and causes the port to transition to the authorized state without any authentication exchange required. The port resends and receives normal traffic without 802.1x-based authentication of the client.

- **force-unauthorized** — Denies all access through this interface by forcing the port to transition to the unauthorized state and ignoring all attempts by the client to authenticate. The device cannot provide authentication services to the client through the interface.

Default Configuration

Port is in the force-authorized state

Command Mode

Interface Configuration (Ethernet)

Command Usage

It is recommended to disable spanning tree or to enable spanning-tree PortFast mode on 802.1x edge ports (ports in auto state that are connected to end stations), in order to get immediately to the forwarding state after successful authentication.

Example

The following command enables 802.1x authentication on Ethernet port 1/e16.

```
Console(config)# interface ethernet 1/e16
Console(config-if)# dot1x port-control auto
```
**dot1x re-authentication**

The `dot1x re-authentication` Interface Configuration mode command enables periodic re-authentication of the client. To return to the default configuration, use the **no** form of this command.

**Syntax**

```
dot1x re-authentication
no dot1x re-authentication
```

**Parameters**

There are no parameters for this command.

**Default Setting**

Periodic re-authentication is disabled.

**Command Mode**

Interface Configuration (Ethernet)

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command enables periodic re-authentication of the client.

```
Console(config)# interface ethernet 1/e16
Console(config-if)# dot1x re-authentication
```
dot1x timeout re-authperiod

The dot1x timeout re-authperiod Interface Configuration mode command sets the number of seconds between re-authentication attempts. To return to the default configuration, use the no form of this command.

Syntax

dot1x timeout re-authperiod seconds
no dot1x timeout re-authperiod

Parameters

- seconds — Number of seconds between re-authentication attempts.
  (Range: 300-4294967295)

Default Setting

Re-authentication period is 3600 seconds.

Command Mode

Interface Configuration (Ethernet) mode

Command Usage

There are no user guidelines for this command.

Example

The following command sets the number of seconds between re-authentication attempts, to 300.

```
Console(config)# interface ethernet 1/e16
Console(config-if)# dot1x timeout re-authperiod 300
```
**dot1x re-authenticate**

The **dot1x re-authenticate** Privileged EXEC mode command manually initiates a re-authentication of all 802.1x-enabled ports or the specified 802.1x-enabled port.

**Syntax**

```
dot1x re-authenticate [ethernet interface]
```

**Parameters**

- **interface** — Valid Ethernet port. (Full syntax: `port`)

**Default Setting**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command manually initiates a re-authentication of 802.1x-enabled Ethernet port 1/e16.

```
Console# dot1x re-authenticate ethernet 1/e16
```
**dot1x timeout quiet-period**

The `dot1x timeout quiet-period` Interface Configuration mode command sets the number of seconds that the device remains in the quiet state following a failed authentication exchange (for example, the client provided an invalid password). To return to the default configuration, use the `no` form of this command.

**Syntax**

```
dot1x timeout quiet-period seconds
no dot1x timeout quiet-period
```

**Parameters**

- `seconds` — Specifies the time in seconds that the device remains in the quiet state following a failed authentication exchange with the client. (Range: 0-65535 seconds)

**Default Setting**

The default quiet period is 60 seconds.

**Command Mode**

Interface Configuration (Ethernet) mode

**Command Usage**

During the quiet period, the device does not accept or initiate authentication requests.

The default value of this command should only be changed to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

To provide a faster response time to the user, a smaller number than the default value should be entered.

**Example**

In the following example, the number of seconds that the device remains in the quiet state following a failed authentication exchange, is set to 3600.

```
Console(config)# interface ethernet 1/e16
Console(config-if)# dot1x timeout quiet-period 3600
```
**dot1x timeout tx-period**

The `dot1x timeout tx-period` Interface Configuration mode command sets the number of seconds that the device waits for a response to an Extensible Authentication Protocol (EAP)-request/identity frame from the client before resending the request. To return to the default configuration, use the `no` form of this command.

**Syntax**

`dot1x timeout tx-period seconds`

`no dot1x timeout tx-period`

**Parameters**

- `seconds` — Specifies the time in seconds that the device waits for a response to an EAP-request/identity frame from the client before resending the request.
  (Range: 1-65535 seconds)

**Default Configuration**

Timeout period is 30 seconds.

**Command Mode**

Interface Configuration (Ethernet) mode

**Command Usage**

The default value of this command should be changed only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

**Example**

The following command sets the number of seconds that the device waits for a response to an EAP-request/identity frame, to 3600 seconds.

```
Console(config)# interface ethernet 1/e16
Console(config-if)# dot1x timeout tx-period 3600
```
**dot1x max-req**

The `dot1x max-req` Interface Configuration mode command sets the maximum number of times that the device sends an Extensible Authentication Protocol (EAP)-request/identity frame (assuming that no response is received) to the client, before restarting the authentication process. To return to the default configuration, use the `no` form of this command.

**Syntax**

```
dot1x max-req count
no dot1x max-req
```

**Parameters**

- `count` — Number of times that the device sends an EAP-request/identity frame before restarting the authentication process. (Range: 1-10)

**Default Configuration**

The default number of times is 2.

**Command Mode**

Interface Configuration (Ethernet) mode

**Command Usage**

The default value of this command should be changed only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

**Example**

The following command sets the number of times that the device sends an EAP-request or identity frame, to 6.

```
Console(config)# interface ethernet 1/e16
Console(config-if)# dot1x max-req 6
```
**dot1x timeout supp-timeout**

The `dot1x timeout supp-timeout` Interface Configuration mode command sets the time for the retransmission of an Extensible Authentication Protocol (EAP)-request frame to the client. To return to the default configuration, use the **no** form of this command.

**Syntax**

```
dot1x timeout supp-timeout seconds
no dot1x timeout supp-timeout
```

**Parameters**

- `seconds` — Time in seconds that the device waits for a response to an EAP-request frame from the client before resending the request. (Range: 1-65535 seconds)

**Default Configuration**

Default timeout period is 30 seconds.

**Command Mode**

Interface configuration (Ethernet) mode

**Command Usage**

The default value of this command should be changed only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

**Example**

The following command sets the timeout period before retransmitting an EAP-request frame to the client to 3600 seconds.

```
Console(config-if)# dot1x timeout supp-timeout 3600
```
**dot1x timeout server-timeout**

The `dot1x timeout server-timeout` Interface Configuration mode command sets the time that the device waits for a response from the authentication server. To return to the default configuration, use the `no` form of this command.

**Syntax**

```plaintext
dot1x timeout server-timeout seconds
no dot1x timeout server-timeout
```

**Parameters**

- `seconds` — Time in seconds that the device waits for a response from the authentication server. (Range: 1-65535 seconds)

**Default Configuration**

The timeout period is 30 seconds.

**Command Mode**

Interface configuration (Ethernet) mode

**Command Usage**

The actual timeout can be determined by comparing the `dot1x timeout server-timeout` value and the result of multiplying the `radius-server retransmit` value with the `radius-server timeout` value and selecting the lower of the two values.

**Example**

The following command sets the time for the retransmission of packets to the authentication server to 3600 seconds.

```plaintext
Console(config-if)# dot1x timeout server-timeout 3600
```
show dot1x

The `show dot1x` Privileged EXEC mode command displays the 802.1x status of the device or specified interface.

**Syntax**

```
show dot1x [ethernet interface]
```

**Parameters**

- `interface` — Valid Ethernet port. (Full syntax: `port`)

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command displays the status of 802.1x-enabled Ethernet ports.

```console
Console# show dot1x

802.1x is enabled

<table>
<thead>
<tr>
<th>Port</th>
<th>Admin Mode</th>
<th>Oper Mode</th>
<th>Reauth Control</th>
<th>Reauth Period</th>
<th>Username</th>
</tr>
</thead>
<tbody>
<tr>
<td>----</td>
<td>----------</td>
<td>--------------</td>
<td>----------------</td>
<td>---------------</td>
<td>----------</td>
</tr>
<tr>
<td>1/e1</td>
<td>Auto</td>
<td>Authorized</td>
<td>Ena</td>
<td>3600</td>
<td>Bob</td>
</tr>
<tr>
<td>1/e2</td>
<td>Auto</td>
<td>Authorized</td>
<td>Ena</td>
<td>3600</td>
<td>John</td>
</tr>
<tr>
<td>1/e3</td>
<td>Auto</td>
<td>Unauthorized</td>
<td>Ena</td>
<td>3600</td>
<td>Clark</td>
</tr>
<tr>
<td>1/e4</td>
<td>Force-auth</td>
<td>Authorized</td>
<td>Dis</td>
<td>3600</td>
<td>n/a</td>
</tr>
<tr>
<td>1/e5</td>
<td>Force-auth</td>
<td>Unauthorized*</td>
<td>Dis</td>
<td>3600</td>
<td>n/a</td>
</tr>
</tbody>
</table>

* Port is down or not present.

Console# show dot1x ethernet 1/e3

802.1x is enabled.

<table>
<thead>
<tr>
<th>Port</th>
<th>Admin Mode</th>
<th>Oper Mode</th>
<th>Reauth Control</th>
<th>Reauth Period</th>
<th>Username</th>
</tr>
</thead>
<tbody>
<tr>
<td>----</td>
<td>----------</td>
<td>---------</td>
<td>----------------</td>
<td>---------------</td>
<td>----------</td>
</tr>
<tr>
<td>1/e3</td>
<td>Auto</td>
<td>Unauthorized</td>
<td>Ena</td>
<td>3600</td>
<td>Clark</td>
</tr>
</tbody>
</table>
```
The following table describes significant fields shown in the example:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>The port number.</td>
</tr>
<tr>
<td>Admin mode</td>
<td>The port admin mode. Possible values: FoTrce-auth, Force-unauth, Auto.</td>
</tr>
<tr>
<td>Oper mode</td>
<td>The port oper mode. Possible values: Authorized, Unauthorized or Down.</td>
</tr>
<tr>
<td>Reauth Control</td>
<td>Reauthentication control.</td>
</tr>
<tr>
<td>Reauth Period</td>
<td>Reauthentication period.</td>
</tr>
<tr>
<td>Username</td>
<td>The username representing the identity of the Supplicant. This field shows</td>
</tr>
<tr>
<td></td>
<td>the username in case the port control is auto. If the port is Authorized,</td>
</tr>
<tr>
<td></td>
<td>it shows the username of the current user. If the port is unauthorized it</td>
</tr>
<tr>
<td></td>
<td>shows the last user that was authenticated successfully.</td>
</tr>
<tr>
<td>Quiet period</td>
<td>The number of seconds that the device remains in the quiet state following</td>
</tr>
<tr>
<td></td>
<td>a failed authentication exchange (for example, the client provided an</td>
</tr>
<tr>
<td></td>
<td>invalid password).</td>
</tr>
<tr>
<td>Tx period</td>
<td>The number of seconds that the device waits for a response to an Extensible</td>
</tr>
<tr>
<td></td>
<td>Authentication Protocol (EAP)-request/identity frame from the client before</td>
</tr>
<tr>
<td></td>
<td>resending the request.</td>
</tr>
<tr>
<td>Max req</td>
<td>The maximum number of times that the device sends an Extensible Authentication</td>
</tr>
<tr>
<td></td>
<td>Protocol (EAP)-request frame (assuming that no response is received) to the</td>
</tr>
<tr>
<td></td>
<td>client before restarting the authentication process.</td>
</tr>
<tr>
<td>Supplicant timeout</td>
<td>Time in seconds the switch waits for a response to an EAP-request frame</td>
</tr>
<tr>
<td></td>
<td>from the client before resending the request.</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
Server timeout | Time in seconds the switch waits for a response from the authentication server before resending the request.
Session Time | The amount of time the user is logged in.
MAC address | The supplicant MAC address.
Authentication Method | The authentication method used to establish the session.
Termination Cause | The reason for the session termination.
State | The current value of the Authenticator PAE state machine and of the Backend state machine.
Authentication success | The number of times the state machine received a Success message from the Authentication Server.
Authentication fails | The number of times the state machine received a Failure message from the Authentication Server.
**show dot1x users**

The **show dot1x users** Privileged EXEC mode command displays active 802.1x authenticated users for the device.

**Syntax**

`show dot1x users [username username]`

**Parameters**

- **username** — Supplicant username (Range: 1-160 characters)

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following commands display 802.1x users.

```
Console# show dot1x users

<table>
<thead>
<tr>
<th>Port</th>
<th>Username</th>
<th>Session Time</th>
<th>Auth Method</th>
<th>MAC Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>-----</td>
<td>----------</td>
<td>--------------</td>
<td>-------------</td>
<td>-------------</td>
</tr>
<tr>
<td>1/e1</td>
<td>Bob</td>
<td>1d:03:08.58</td>
<td>Remote</td>
<td>0008:3b79:8787</td>
</tr>
<tr>
<td>1/e2</td>
<td>John</td>
<td>08:19:17</td>
<td>None</td>
<td>0008:3b89:3127</td>
</tr>
</tbody>
</table>

Console# show dot1x users username Bob

User name: Bob

<table>
<thead>
<tr>
<th>Port</th>
<th>Username</th>
<th>Session Time</th>
<th>Auth Method</th>
<th>MAC Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>-----</td>
<td>----------</td>
<td>--------------</td>
<td>-------------</td>
<td>-------------</td>
</tr>
<tr>
<td>1/e1</td>
<td>Bob</td>
<td>1d:03:08.58</td>
<td>Remote</td>
<td>0008:3b79:8787</td>
</tr>
</tbody>
</table>
```

The following table describes the significant fields shown in the example:

<table>
<thead>
<tr>
<th><strong>Keyword</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>The port number.</td>
</tr>
<tr>
<td>Username</td>
<td>The username representing the identity of the Supplicant.</td>
</tr>
<tr>
<td>Session Time</td>
<td>The period of time the Supplicant is connected to the system.</td>
</tr>
<tr>
<td>Authentication Method</td>
<td>Authentication method used by the Supplicant to open the session.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>MAC address of the Supplicant.</td>
</tr>
</tbody>
</table>
show dot1x statistics

The `show dot1x statistics` Privileged EXEC mode command displays 802.1x statistics for the specified interface.

**Syntax**

`show dot1x statistics ethernet interface`

**Parameters**

- **interface** — Valid Ethernet port. (Full syntax: `port`)

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command displays 802.1x statistics for the specified interface.

```
Console# show dot1x statistics ethernet 1/e1

EapolFramesRx: 11
EapolFramesTx: 12
EapolStartFramesRx: 12
EapolLogoffFramesRx: 1
EapolRespIdFramesRx: 3
EapolRespFramesRx: 6
EapolReqIdFramesTx: 3
EapolReqFramesTx: 6
InvalidEapolFramesRx: 0
EapLengthErrorFramesRx: 0
LastEapolFrameVersion: 1
LastEapolFrameSource: 00:08:78:32:98:78
```

The following table describes the significant fields shown in the example:

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EapolFramesRx</td>
<td>The number of valid EAPOL frames of any type that have been received by this Authenticator.</td>
</tr>
<tr>
<td>EapolFramesTx</td>
<td>The number of EAPOL frames of any type that have been transmitted by this Authenticator.</td>
</tr>
<tr>
<td>Keyword</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>EapolStartFramesRx</td>
<td>The number of EAPOL Start frames that have been received by this Authenticator.</td>
</tr>
<tr>
<td>EapolLogoffFramesRx</td>
<td>The number of EAPOL Logoff frames that have been received by this Authenticator.</td>
</tr>
<tr>
<td>EapolRespIdFramesRx</td>
<td>The number of EAP Resp/Id frames that have been received by this Authenticator.</td>
</tr>
<tr>
<td>EapolRespFramesRx</td>
<td>The number of valid EAP Response frames (other than Resp/Id frames) that have been received by this Authenticator.</td>
</tr>
<tr>
<td>EapolReqIdFramesTx</td>
<td>The number of EAP Req/Id frames that have been transmitted by this Authenticator.</td>
</tr>
<tr>
<td>EapolReqFramesTx</td>
<td>The number of EAP Request frames (other than Rq/Id frames) that have been transmitted by this Authenticator.</td>
</tr>
<tr>
<td>InvalidEapolFramesRx</td>
<td>The number of EAPOL frames that have been received by this Authenticator in which the frame type is not recognized.</td>
</tr>
<tr>
<td>EapLengthErrorFramesRx</td>
<td>The number of EAPOL frames that have been received by this Authenticator in which the Packet Body Length field is invalid.</td>
</tr>
<tr>
<td>LastEapolFrameVersion</td>
<td>The protocol version number carried in the most recently received EAPOL frame.</td>
</tr>
<tr>
<td>LastEapolFrameSource</td>
<td>The source MAC address carried in the most recently received EAPOL frame.</td>
</tr>
</tbody>
</table>
Advanced Features

dot1x auth-not-req

The **dot1x auth-not-req** Interface Configuration mode command enables unauthorized devices access to the VLAN. To disable access to the VLAN, use the **no** form of this command.

**Syntax**

dot1x auth-not-req

no dot1x auth-not-req

**Parameters**

There are no parameters for this command.

**Default Configuration**

Access is enabled.

**Command Mode**

Interface Configuration (VLAN) mode

**Command Usage**

An access port cannot be a member in an unauthenticated VLAN.

The native VLAN of a trunk port cannot be an unauthenticated VLAN.

For a general port, the PVID can be an unauthenticated VLAN (although only tagged packets would be accepted in the unauthorized state.)

**Example**

The following command enables access to the VLAN to unauthorized devices.

```
Console(config-if)# dot1x auth-not-req
```
**802.1x Commands**

**dot1x multiple-hosts**

The **dot1x multiple-hosts** Interface Configuration mode command enables multiple hosts (clients) on an 802.1x-authorized port, where the authorization state of the port is set to **auto**. To return to the default configuration, use the **no** form of this command.

### Syntax

```
dot1x multiple-hosts
```

```
no dot1x multiple-hosts
```

### Parameters

There are no parameters for this command.

### Default Configuration

Multiple hosts are disabled.

### Command Mode

Interface Configuration (Ethernet) mode

### Command Usage

This command enables the attachment of multiple clients to a single 802.1x-enabled port. In this mode, only one of the attached hosts must be successfully authorized for all hosts to be granted network access. If the port becomes unauthorized, all attached clients are denied access to the network.

For unauthenticated VLANs, multiple hosts are always enabled.

Multiple-hosts must be enabled to enable port security on the port.

### Example

The following command enables multiple hosts (clients) on an 802.1x-authorized port.

```
Console(config-if)# dot1x multiple-hosts
```
dot1x single-host-violation

The `dot1x single-host-violation` Interface Configuration mode command configures the action to be taken, when a station whose MAC address is not the supplicant MAC address, attempts to access the interface. Use the `no` form of this command to return to default.

**Syntax**

dot1x single-host-violation {forward | discard | discard-shutdown} [trap seconds]

no port dot1x single-host-violation

**Parameters**

- **forward** — Forwards frames with source addresses that are not the supplicant address, but does not learn the source addresses.
- **discard** — Discards frames with source addresses that are not the supplicant address.
- **discard-shutdown** — Discards frames with source addresses that are not the supplicant address. The port is also shut down.
- **trap** — Indicates that SNMP traps are sent.
- **seconds** — Specifies the minimum amount of time in seconds between consecutive traps. (Range: 1-1000000)

**Default Setting**

Frames with source addresses that are not the supplicant address are discarded.

No traps are sent.

**Command Mode**

Interface Configuration (Ethernet) mode

**Command Usage**

The command is relevant when multiple hosts is disabled and the user has been successfully authenticated.

**Example**

The following command forwards frames with source addresses that are not the supplicant address and sends consecutive traps at intervals of 100 seconds.

```
Console(config-if)# dot1x single-host-violation forward trap 100
```
**dot1x guest-vlan**

The **dot1x guest-vlan** Interface Configuration mode command defines a guest VLAN. To return to the default configuration, use the **no** form of this command.

**Syntax**

dot1x guest-vlan  
no dot1x guest-vlan

**Parameters**

There are no parameters for this command.

**Default Setting**

No VLAN is defined as a guest VLAN.

**Command Mode**

Interface Configuration (VLAN) mode

**Command Usage**

Use the **dot1x guest-vlan enable** Interface Configuration mode command to enable unauthorized users on an interface to access the guest VLAN.

If the guest VLAN is defined and enabled, the port automatically joins the guest VLAN when the port is unauthorized and leaves it when the port becomes authorized. To be able to join or leave the guest VLAN, the port should not be a static member of the guest VLAN.

**Example**

The following command defines VLAN 2 as a guest VLAN.

```
Console#  
Console# configure
Console(config)# vlan database  
Console(config-vlan)# vlan 2  
Console(config-vlan)# exit
Console(config)# interface vlan 2  
Console(config-if)# dot1x guest-vlan
```
### dot1x guest-vlan enable

The **dot1x vlans guest-vlan enable** Interface Configuration mode command enables unauthorized users on the interface access to the Guest VLAN. To disable access, use the **no** form of this command.

**Syntax**

```
dot1x guest-vlan enable
no dot1x guest-vlan enable
```

**Parameters**

There are no parameters for this command.

**Default Setting**

Disabled.

**Command Mode**

Interface Configuration (Ethernet) mode

**Command Usage**

A device can have only one global guest VLAN. The guest VLAN is defined using the **dot1x guest-vlan** Interface Configuration mode command.

**Example**

The following command enables unauthorized users on Ethernet port 1/e1 to access the guest VLAN.

```
Console# configure
Console(config)# interface ethernet 1/e1
Console(config-if)# dot1x guest-vlan enable
```
**show dot1x advanced**

The **show dot1x advanced** Privileged EXEC mode command displays 802.1x advanced features for the device or specified interface.

**Syntax**

```
show dot1x advanced [ethernet interface]
```

**Parameters**

- **interface** — Valid Ethernet port. (Full syntax: `port`)

**Default Setting**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command displays 802.1x advanced features for the device.

```
Console# show dot1x advanced

Guest VLAN: 2
Unauthenticated VLANs: 91,92

Interface     Multiple Hosts     Guest VLAN
-------------- ----------- -----------
1/e1          Disabled          Enabled
1/e2          Enabled           Disabled

Console# show dot1x advanced ethernet 1/e1

Interface         Multiple Hosts     Guest VLAN
--------------- ----------- -----------
1/e1             Disabled          Enabled

Single host parameters
Violation action: Discard
Trap: Enabled
Trap frequency: 100
Status: Single-host locked
Violations since last trap: 9
```
aaa authentication login

The **aaa authentication login** Global Configuration mode command defines login authentication. To return to the default configuration, use the **no** form of this command.

**Syntax**

```
aaa authentication login {default | list-name} method1 [method2...]
```

```
no aaa authentication login {default | list-name}
```

**Parameters**

- **default** — Uses the listed authentication methods that follow this argument as the default list of methods when a user logs in.
- **list-name** — Character string used to name the list of authentication methods activated when a user logs in. (Range: 1-12 characters).
- **method1 [method2...]** — Specify at least one from the following table:

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Uses the enable password for authentication.</td>
</tr>
<tr>
<td>line</td>
<td>Uses the line password for authentication.</td>
</tr>
<tr>
<td>none</td>
<td>Uses no authentication.</td>
</tr>
<tr>
<td>radius</td>
<td>Uses the list of all RADIUS servers for authentication.</td>
</tr>
<tr>
<td>tacacs</td>
<td>Uses the list of all TACACS+ servers for authentication.</td>
</tr>
</tbody>
</table>

**Default Setting**

The local user database is checked. This has the same effect as the command **aaa authentication login list-name local**.

On the console, login succeeds without any authentication check if the authentication method is not defined.

**Command Mode**

Global Configuration mode

**Command Usage**

The default and optional list names created with the **aaa authentication login** command are used with the **login authentication** command.
Create a list by entering the `aaa authentication login list-name method` command for a particular protocol, where `list-name` is any character string used to name this list. The `method` argument identifies the list of methods that the authentication algorithm tries, in the given sequence.

The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify `none` as the final method in the command line.

**Example**

The following command configures the authentication login.

```
Console(config)# aaa authentication login default radius local enable none
```
aaa authentication enable

The **aaa authentication enable** Global Configuration mode command defines authentication method lists for accessing higher privilege levels. To return to the default configuration, use the **no** form of this command.

**Syntax**

```
caaa authentication enable {default | list-name} method1 [method2...]
```

```
no aaa authentication enable {default | list-name}
```

**Parameters**

- **default** — Uses the listed authentication methods that follow this argument as the default list of methods, when using higher privilege levels.
- **list-name** — Character string used to name the list of authentication methods activated, when using access higher privilege levels (Range: 1-12 characters).
- **method1 [method2...]** — Specify at least one keyword from the following table:

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Uses the enable password for authentication.</td>
</tr>
<tr>
<td>line</td>
<td>Uses the line password for authentication.</td>
</tr>
<tr>
<td>none</td>
<td>Uses no authentication.</td>
</tr>
<tr>
<td>radius</td>
<td>Uses the list of all RADIUS servers for authentication. Uses username $enabx$., where x is the privilege level.</td>
</tr>
<tr>
<td>tacacs</td>
<td>Uses the list of all TACACS+ servers for authentication. Uses username &quot;$enabx$.&quot; where x is the privilege level.</td>
</tr>
</tbody>
</table>

**Default Setting**

If the **default** list is not set, only the enable password is checked. This has the same effect as the command **aaa authentication enable default enable**.

On the console, the enable password is used if it exists. If no password is set, the process still succeeds. This has the same effect as using the command **aaa authentication enable default enable none**.

**Command Mode**

Global Configuration mode

**Command Usage**

The default and optional list names created with the **aaa authentication enable** command are used with the **enable authentication** command.

The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify **none** as the final method in the command line.

All **aaa authentication enable default** requests sent by the device to a RADIUS or TACACS+ server include the username $enabx$., where x is the requested privilege level.
Example

The following command sets the enable password for authentication when accessing higher privilege levels.

```
Console(config)# aaa authentication enable default enable
```
**login authentication**

The `login authentication` Line Configuration mode command specifies the login authentication method list for a remote telnet or console. To return to the default configuration specified by the `aaa authentication login` command, use the `no` form of this command.

**Syntax**

```
login authentication {default | list-name}
no login authentication
```

**Parameters**

- `default` — Uses the default list created with the `aaa authentication login` command.
- `list-name` — Uses the indicated list created with the `aaa authentication login` command.

**Default Setting**

Uses the default set with the command `aaa authentication login`.

**Command Mode**

Line Configuration mode

**Command Usage**

Changing login authentication from default to another value may disconnect the telnet session.

**Example**

The following command specifies the default authentication method for a console.

```
Console(config)# line console
Console(config-line)# login authentication default
```
enable authentication

The `enable authentication` Line Configuration mode command specifies the authentication method list when accessing a higher privilege level from a remote telnet or console. To return to the default configuration specified by the `aaa authentication enable` command, use the `no` form of this command.

**Syntax**

```plaintext
enable authentication {default | list-name}
no enable authentication
```

**Parameters**

- `default` — Uses the default list created with the `aaa authentication enable` command.
- `list-name` — Uses the indicated list created with the `aaa authentication enable` command.

**Default Setting**

Uses the default set with the `aaa authentication enable` command.

**Command Mode**

Line Configuration mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command specifies the default authentication method when accessing a higher privilege level from a console.

```
Console(config)# line console
Console(config-line)# enable authentication default
```
ip http authentication

The `ip http authentication` Global Configuration mode command specifies authentication methods for HTTP server users. To return to the default configuration, use the `no` form of this command.

**Syntax**

```
ip http authentication method1 [method2...]
nop ip http authentication
```

**Parameters**

- `method1 [method2...]` — Specify at least one from the following table:

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>local</td>
<td>Uses the local username database for authentication.</td>
</tr>
<tr>
<td>none</td>
<td>Uses no authentication.</td>
</tr>
<tr>
<td>radius</td>
<td>Uses the list of all RADIUS servers for authentication.</td>
</tr>
<tr>
<td>tacacs</td>
<td>Uses the list of all TACACS+ servers for authentication.</td>
</tr>
</tbody>
</table>

**Default Setting**

The local user database is checked. This has the same effect as the command `ip http authentication local`.

**Command Mode**

Global Configuration mode

**Command Usage**

The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify `none` as the final method in the command line.

**Example**

The following command configures the HTTP authentication.

```
Console(config)# ip http authentication radius local
```
ip https authentication

The ip https authentication Global Configuration mode command specifies authentication methods for HTTPS server users. To return to the default configuration, use the no form of this command.

**Syntax**

```
ip https authentication method1 [method2...]
```

no ip https authentication

**Parameters**

- **method1 [method2...]** — Specify at least one from the following table:

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Source or Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>local</td>
<td>Uses the local username database for authentication.</td>
</tr>
<tr>
<td>none</td>
<td>Uses no authentication.</td>
</tr>
<tr>
<td>radius</td>
<td>Uses the list of all RADIUS servers for authentication.</td>
</tr>
<tr>
<td>tacacs</td>
<td>Uses the list of all TACACS+ servers for authentication.</td>
</tr>
</tbody>
</table>

**Default Setting**

The local user database is checked. This has the same effect as the command ip https authentication local.

**Command Mode**

Global Configuration mode

**Command Usage**

The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify none as the final method in the command line.

**Example**

The following command configures HTTPS authentication.

```
Console(config)# ip https authentication radius local
```
**show authentication methods**

The **show authentication methods** privileged EXEC mode command displays information about the authentication methods.

**Syntax**

`show authentication methods`

**Parameters**

There are no parameters for this command.

**Default Setting**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command displays the authentication configuration.

```
Console# show authentication methods

---------------------------------
Default: RADIUS, Local, Line
Console_Login: Line, None

Enable Authentication Method Lists
----------------------------------
Default: RADIUS, Enable
Console_Enable: Enable, None

<table>
<thead>
<tr>
<th>Line</th>
<th>Login Method List</th>
<th>Enable Method List</th>
</tr>
</thead>
<tbody>
<tr>
<td>Console</td>
<td>Console_Login</td>
<td>Console_Enable</td>
</tr>
<tr>
<td>Telnet</td>
<td>Default</td>
<td>Default</td>
</tr>
<tr>
<td>SSH</td>
<td>Default</td>
<td>Default</td>
</tr>
</tbody>
</table>

http: RADIUS, Local
https: RADIUS, Local
dot1x: RADIUS
```
The **password** Line Configuration mode command specifies a password on a line. To remove the password, use the **no** form of this command.

**Syntax**

```
password password [encrypted]
no password
```

**Parameters**

- **password** — Password for this level (Range: 1-160 characters).
- **encrypted** — Encrypted password to be entered, copied from another device configuration.

**Default Setting**

No password is defined.

**Command Mode**

Line Configuration mode

**Command Usage**

If a password is defined as encrypted, the required password length is 32 characters.

**Example**

The following command specifies password **secret** on a console.

```
Console(config)# line console
Console(config-line)# password secret
```
enable password

The `enable password` Global Configuration mode command sets a local password to control access to user and privilege levels. To remove the password requirement, use the `no` form of this command.

**Syntax**

```plaintext
enable password [level level] password [encrypted]
no enable password [level level]
```

**Parameters**

- `password` — Password for this level (Range: 1-159 characters).
- `level` — The user privilege level with the following options:
  - 1 — Allows access but not configuration rights.
  - 15 — Enables access and configuration rights.
- `encrypted` — Encrypted password entered, copied from another device configuration.

**Default Configuration**

No enable password is defined.

**Command Mode**

Global Configuration mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following example sets local level 15 password secret to control access to user and privilege levels.

```
Console(config)# enable password level 15 secret
```
username

The **username** Global Configuration mode command creates a user account in the local database. To remove a user name, use the **no** form of this command.

**Syntax**

```
username name [password password] [level level] [encrypted]
no username name
```

**Parameters**

- **name** — The name of the user (Range: 1-20 characters).
- **password** — The authentication password for the user (Range: 1-159 characters).
- **level** — The user privilege level with the following options:
  - 1 — Allows access but not configuration rights.
  - 15 — Enables access and configuration rights.
- **encrypted** — Encrypted password entered, copied from another device configuration.

**Default Configuration**

No user is defined.

**Command Mode**

Global Configuration mode

**Command Usage**

User account can be created without a password.

**Example**

The following example configures user bob with password lee and user level 15 to the system.

```
Console(config)# username bob password lee level 15
```
ip access-list

The ip access-list Global Configuration command enables the IP-Access Configuration mode and creates Layer 3 ACLs. To delete an ACL, use the no form of this command.

Syntax

```
ip access-list name
no ip access-list name
```

Parameters

■ name — Specifies the name of the ACL.

Default Setting

The default for all ACLs is deny-all.

Command Mode

Global Configuration mode

Command Usage

Up to 1018 rules can be defined on the device, depending on the type of rule defined.

Example

The following command creates an IP ACL.

```
Console(config)# ip access-list ip-acl1
Console(config-ip-al)#
```
### permit (IP)

The **permit** IP-Access List Configuration mode command permits traffic if the conditions defined in the permit statement match.

#### Syntax

```plaintext
permit {any | protocol} {any | {source source-wildcard}} {any | {destination destination-wildcard}} [dscp dscp number | ip-precedence ip-precedence]
permit-icmp {any | {source source-wildcard}} {any | {destination destination-wildcard}} {any | icmp-type} {any | icmp-code} [dscp number | ip-precedence number]
permit-igmp {any | {source source-wildcard}} {any | {destination destination-wildcard}} {any | igmp-type} [dscp number | ip-precedence number]
permit-tcp {any | {source source-wildcard}} {any | source-port} {any | {destination destination-wildcard}} {any | destination-port} [dscp number | ip-precedence number] [flags list-of-flags]
permit-udp {any | {source source-wildcard}} {any | source-port} {any | {destination destination-wildcard}} {any | destination-port} [dscp number | ip-precedence number]
```

#### Parameters

- **source** — Specifies the source IP address of the packet. Specify **any** to indicate IP address 0.0.0.0 and mask 255.255.255.255.
- **source-wildcard** — Specifies wildcard to be applied to the source IP address. Use 1s in bit positions to be ignored. Specify **any** to indicate IP address 0.0.0.0 and mask 255.255.255.255.
- **destination** — Specifies the destination IP address of the packet. Specify **any** to indicate IP address 0.0.0.0 and mask 255.255.255.255.
- **destination-wildcard** — Specifies wildcard to be applied to the destination IP address. Use 1s in bit positions to be ignored. Specify **any** to indicate IP address 0.0.0.0 and mask 255.255.255.255.
- **protocol** — Specifies the abbreviated name or number of an IP protocol. (Range: 0-255)

The following table lists protocols that can be specified:

<table>
<thead>
<tr>
<th>IP Protocol</th>
<th>Abbreviated Name</th>
<th>Protocol Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Control Message Protocol</td>
<td>icmp</td>
<td>1</td>
</tr>
<tr>
<td>Internet Group Management Protocol</td>
<td>igmp</td>
<td>2</td>
</tr>
<tr>
<td>IP in IP (encapsulation) Protocol</td>
<td>ipinip</td>
<td>4</td>
</tr>
<tr>
<td>Transmission Control Protocol</td>
<td>tcp</td>
<td>6</td>
</tr>
<tr>
<td>Exterior Gateway Protocol</td>
<td>egp</td>
<td>8</td>
</tr>
<tr>
<td>Interior Gateway Protocol</td>
<td>igp</td>
<td>9</td>
</tr>
<tr>
<td>User Datagram Protocol</td>
<td>udp</td>
<td>17</td>
</tr>
<tr>
<td>Host Monitoring Protocol</td>
<td>hmp</td>
<td>20</td>
</tr>
<tr>
<td>Reliable Data Protocol</td>
<td>rdp</td>
<td>27</td>
</tr>
<tr>
<td>Inter-Domain Policy Routing Protocol</td>
<td>idpr</td>
<td>35</td>
</tr>
</tbody>
</table>
### ACL Commands

- **DSCP** — Indicates matching the dscp number with the packet DSCP value.
- **ip-precedence** — Indicates matching ip-precedence with the packet ip-precedence value.
- **icmp-type** — Specifies an ICMP message type for filtering ICMP packets. Enter a value or one of the following values: `echo-reply`, `destination-unreachable`, `source-quench`, `redirect`, `alternate-host-address`, `echo-request`, `router-advertisement`, `router-solicitation`, `time-exceeded`, `parameter-problem`, `timestamp`, `timestamp-reply`, `information-request`, `information-reply`, `address-mask-request`, `address-mask-reply`, `traceroute`, `datagram-conversion-error`, `mobile-host-redirect`, `ipv6-where-are-you`, `ipv6-i-am-here`, `mobile-registration-request`, `mobile-registration-reply`, `domain-name-request`, `domain-name-reply`, `address-mask-request`, `address-mask-reply`. (Range: 0-255)
- **icmp-code** — Specifies an ICMP message code for filtering ICMP packets. ICMP packets that are filtered by ICMP message type can also be filtered by the ICMP message code. (Range: 0-255)
- **igmp-type** — IGMP packets can be filtered by IGMP message type. Enter a number or one of the following values: `dvMrp`, `host-query`, `host-report`, `pim` or `trace`, `host-report-v2`, `host-leave-v2`, `host-report-v3` (Range: 0-255)
- **destination-port** — Specifies the UDP/TCP destination port. (Range: 0-65535)
- **source-port** — Specifies the UDP/TCP source port. (Range: 0-65535)
- **list-of-flags** — Specifies a list of TCP flags that can be triggered. If a flag is set, it is prefixed by “+”. If a flag is not set, it is prefixed by “-”. Possible values: `+urg`, `+ack`, `+psh`, `+rst`, `+syn`, `+fin`, `-urg`, `-ack`, `-psh`, `-rst`, `-syn` and `-fin`. The flags are concatenated into one string. For example: `+fin-ack`.

<table>
<thead>
<tr>
<th>IP Protocol</th>
<th>Abbreviated Name</th>
<th>Protocol Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ipv6 Protocol</td>
<td>ipv6</td>
<td>41</td>
</tr>
<tr>
<td>Routing Header for Ipv6</td>
<td>ipv6-route</td>
<td>43</td>
</tr>
<tr>
<td>Fragment Header for Ipv6</td>
<td>ipv6-frag</td>
<td>44</td>
</tr>
<tr>
<td>Inter-Domain Routing Protocol</td>
<td>idrp</td>
<td>45</td>
</tr>
<tr>
<td>Reservation Protocol</td>
<td>rsvp</td>
<td>46</td>
</tr>
<tr>
<td>General Routing Encapsulation</td>
<td>gre</td>
<td>47</td>
</tr>
<tr>
<td>Encapsulating Security Payload (50)</td>
<td>esp</td>
<td>50</td>
</tr>
<tr>
<td>Authentication Header</td>
<td>ah</td>
<td>51</td>
</tr>
<tr>
<td>ICM for Ipv6 Protocol</td>
<td>ipv6-icmp</td>
<td>58</td>
</tr>
<tr>
<td>EIGRP Routing Protocol</td>
<td>eigrp</td>
<td>88</td>
</tr>
<tr>
<td>Open Shortest Path Protocol</td>
<td>ospf</td>
<td>89</td>
</tr>
<tr>
<td>Protocol Independent Multicast</td>
<td>pim</td>
<td>103</td>
</tr>
<tr>
<td>Layer Two Tunneling Protocol</td>
<td>l2tp</td>
<td>115</td>
</tr>
<tr>
<td>ISIS over IPv4 Protocol</td>
<td>isis</td>
<td>124</td>
</tr>
<tr>
<td>(any IP protocol)</td>
<td>any</td>
<td>(25504)</td>
</tr>
</tbody>
</table>
**Default Setting**

No IPv4 ACL is defined.

**Command Mode**

IP-Access List Configuration mode

**Command Usage**

Use the `ip access-list` Global Configuration mode command to enable the IP-Access List Configuration mode.

Before an Access Control Element (ACE) is added to an ACL, all packets are permitted. After an ACE is added, an implied `deny-any-any` condition exists at the end of the list and those packets that do not match the conditions defined in the permit statement are denied.

**Example**

The following command define a permit statement for an IP ACL.

```
Console(config)# ip access-list ip-acl1
Console(config-ip-al)# permit rsvp 192.1.1.1 0.0.0.0 any dscp 56
```
deny (IP)

The **deny** IP-Access List Configuration mode command denies traffic if the conditions defined in the deny statement match.

**Syntax**

```plaintext
deny [disable-port] {any | protocol} {any | {source source-wildcard}} {any | {destination destination-wildcard}} [dscp dscp-number | ip-precedence ip-precedence]
deny {any | protocol} {any | {source source-wildcard}} {any | {destination destination-wildcard}} [dscp dscp-number ip-precedence ip-precedence]
deny-icmp {any | {source source-wildcard}} {any | {destination destination-wildcard}} {any | icmp-type} {any | icmp-code} [dscp number ip-precedence number]
deny-igmp {any | {source source-wildcard}} {any | {destination destination-wildcard}} {any | igmp-type} [dscp number ip-precedence number]
```

**Parameters**

- **disable-port** — Specifies that the port should be disabled if the conditions defined match.
- **source** — Specifies the IP address or host name from which the packet was sent. Specify **any** to indicate IP address 0.0.0.0 and mask 255.255.255.255.
- **source-wildcard** — Specifies wildcard bits by placing 1s in bit positions to be ignored. Specify **any** to indicate IP address 0.0.0.0 and mask 255.255.255.255.
- **destination** — Specifies the IP address or host name to which the packet is being sent. Specify **any** to indicate IP address 0.0.0.0 and mask 255.255.255.255.
- **destination-wildcard** — Specifies wildcard bits by placing 1s in bit positions to be ignored. Specify **any** to indicate IP address 0.0.0.0 and mask 255.255.255.255.
- **protocol** — Specifies the abbreviated name or number of an IP protocol.

The following table lists protocols that can be specified:

<table>
<thead>
<tr>
<th>IP Protocol</th>
<th>Abbreviated Name</th>
<th>Protocol Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Control Message Protocol</td>
<td>icmp</td>
<td>1</td>
</tr>
<tr>
<td>Internet Group Management Protocol</td>
<td>igmp</td>
<td>2</td>
</tr>
<tr>
<td>IP in IP (encapsulation) Protocol</td>
<td>ipinip</td>
<td>4</td>
</tr>
<tr>
<td>Transmission Control Protocol</td>
<td>tcp</td>
<td>6</td>
</tr>
<tr>
<td>Exterior Gateway Protocol</td>
<td>egp</td>
<td>8</td>
</tr>
<tr>
<td>Interior Gateway Protocol</td>
<td>igp</td>
<td>9</td>
</tr>
<tr>
<td>User Datagram Protocol</td>
<td>udp</td>
<td>17</td>
</tr>
<tr>
<td>Host Monitoring Protocol</td>
<td>hmp</td>
<td>20</td>
</tr>
<tr>
<td>Reliable Data Protocol</td>
<td>rdp</td>
<td>27</td>
</tr>
<tr>
<td>Inter-Domain Policy Routing Protocol</td>
<td>idpr</td>
<td>35</td>
</tr>
<tr>
<td>IPv6 Protocol</td>
<td>ipv6</td>
<td>41</td>
</tr>
<tr>
<td>Routing Header for IPv6</td>
<td>ipv6-route</td>
<td>43</td>
</tr>
<tr>
<td>Fragment Header for IPv6</td>
<td>ipv6-frag</td>
<td>44</td>
</tr>
</tbody>
</table>
ACL Commands

<table>
<thead>
<tr>
<th>IP Protocol</th>
<th>Abbreviated Name</th>
<th>Protocol Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inter-Domain Routing Protocol</td>
<td>idrp</td>
<td>45</td>
</tr>
<tr>
<td>Reservation Protocol</td>
<td>rsvp</td>
<td>46</td>
</tr>
<tr>
<td>General Routing Encapsulation</td>
<td>gre</td>
<td>47</td>
</tr>
<tr>
<td>Encapsulating Security Payload (50)</td>
<td>esp</td>
<td>50</td>
</tr>
<tr>
<td>Authentication Header</td>
<td>ah</td>
<td>51</td>
</tr>
<tr>
<td>ICMP for IPv6</td>
<td>ipv6-icmp</td>
<td>58</td>
</tr>
<tr>
<td>EIGRP rOuting Protocol</td>
<td>eigrp</td>
<td>88</td>
</tr>
<tr>
<td>Open Shortest Path Protocol</td>
<td>ospf</td>
<td>89</td>
</tr>
<tr>
<td>Protocol Independent Multicast</td>
<td>pim</td>
<td>103</td>
</tr>
<tr>
<td>Layer Two Tunneling Protocol</td>
<td>I2tp</td>
<td>115</td>
</tr>
<tr>
<td>ISIS over IPv4</td>
<td>isis</td>
<td>124</td>
</tr>
<tr>
<td>(any IP protocol)</td>
<td>any</td>
<td>(25504)</td>
</tr>
</tbody>
</table>

- **dscp** — Indicates matching the dscp number with the packet dscp value.
- **ip-precedence** — Indicates matching ip-precedence with the packet ip-precedence value.

**Default Setting**
This command has no default configuration.

**Command Mode**
IP-Access List Configuration mode

**Command Usage**
Use the `ip access-list` Global Configuration mode command to enable the IP-Access List Configuration mode.

Before an Access Control Element (ACE) is added to an ACL, all packets are permitted. After an ACE is added, an implied `deny-any-any` condition exists at the end of the list and those packets that do not match the defined conditions are denied.

**Example**
The following commands define a permit statement for an IP ACL.

```
Console(config)# ip access-list ip-acl1
Console(config-ip-al)# deny rsvp 192.1.1.1 0.0.0.255 any
```
**mac access-list**

The `mac access-list` Global Configuration mode command enables the MAC-Access List Configuration mode and creates Layer 2 ACLs. To delete an ACL, use the `no` form of this command.

**Syntax**

```
mac access-list name
no mac access-list name
```

**Parameters**

- `name` — Specifies the name of the ACL.

**Default Setting**

The default for all ACLs is `deny all`.

**Command Mode**

Global Configuration mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command creates a MAC ACL.

```
Console(config)# mac access-list mac1
Console(config-mac-al)#
```
permit (MAC)

The **permit** MAC-Access List Configuration mode command defines permit conditions of an MAC ACL.

**Syntax**

```
permit {any | {host source source-wildcard} any | {destination destination-wildcard}} [vlan vlan-id] [cos cos cos-wildcard] [ethtype eth-type]
```

**Parameters**

- **source** — Specifies the source MAC address of the packet.
- **source-wildcard** — Specifies wildcard bits to be applied to the source MAC address. Use 1s in bit positions to be ignored.
- **destination** — Specifies the MAC address of the host to which the packet is being sent.
- **destination-wildcard** — Specifies wildcard bits to be applied to the destination MAC address. Use 1s in bit positions to be ignored.
- **vlan-id** — Specifies the ID of the packet VLAN. (Range: 0-4095)
- **cos** — Specifies the Class of Service (CoS) for the packet. (Range: 0-7)
- **cos-wildcard** — Specifies wildcard bits to be applied to the CoS.
- **eth-type** — Specifies the Ethernet type of the packet. (Range: 0-65535)

**Default Setting**

No MAC ACL is defined.

**Command Mode**

MAC-Access List Configuration mode

**Command Usage**

Before an Access Control Element (ACE) is added to an ACL, all packets are permitted. After an ACE is added, an implied **deny-any-any** condition exists at the end of the list and those packets that do not match the conditions defined in the permit statement are denied.

If the VLAN ID is specified, the policy map cannot be connected to the VLAN interface.

**Example**

The following commands create a MAC ACL with permit rules.

```
Console(config)# mac access-list macl-acl1
Console(config-mac-al)# permit 6:6:6:6:6:6 0:0:0:0:0:0 any vlan 6
```
deny (MAC)

The **deny** MAC-Access List Configuration mode command denies traffic if the conditions defined in the deny statement match.

**Syntax**

```
deny destination
```

```
deny [disable-port] {any | {source source-wildcard}} {any | {destination destination-wildcard}} [vlan vlan-id] [cos cos-wildcard] [ethtype eth-type]
```

**Parameters**

- **disable-port** — Indicates that the port is disabled if the statement is deny.
- **source** — Specifies the MAC address of the host from which the packet was sent.
- **source-wildcard** — (Optional for the first type) Specifies wildcard bits by placing 1s in bit positions to be ignored.
- **destination** — Specifies the MAC address of the host to which the packet is being sent.
- **destination-wildcard** — (Optional for the first type) Specifies wildcard bits by placing 1s in bit positions to be ignored.
- **vlan-id** — Specifies the ID of the packet vlan.
- **cos** — Specifies the packets’s Class of Service (CoS).
- **cos-wildcard** — Specifies wildcard bits to be applied to the CoS.
- **eth-type** — Specifies the packet’s Ethernet type.

**Default Setting**

This command has no default configuration.

**Command Mode**

MAC-Access List Configuration mode

**Command Usage**

MAC BPDU packets cannot be denied.

This command defines an Access Control Element (ACE). An ACE can only be removed by deleting the ACL, using the **no mac access-list** Global Configuration mode command. Alternatively, the Web-based interface can be used to delete ACEs from an ACL.

Use the following user guidelines:

- Before an Access Control Element (ACE) is added to an ACL, all packets are permitted. After an ACE is added, an implied **deny-any-any** condition exists at the end of the list and those packets that do not match the conditions defined in the permit statement are denied.

- If the VLAN ID is specified, the policy map cannot be connected to the VLAN interface.
**Example**

The following commands create a MAC ACL with deny rules on a device.

```
Console(config)# mac access-list mac1
Console (config-mac-acl)# deny 06:06:06:06:06:06:00:00:00:00:00:00 any
```
service-acl

The service-acl Interface Configuration mode command applies an ACL to the input interface. To detach an ACL from an input interface, use the no form of this command.

Syntax

service-acl {input acl-name}
no service-acl {input}

Parameters

acl-name — Specifies the ACL to be applied to the input interface.

Default Setting

This command has no default configuration.

Command Mode

Interface (Ethernet, port-channel) Configuration mode.

Example

The following command binds (services) an ACL to VLAN 2.

```
Console(config)# interface vlan 2
Console(config-if)# service-acl input acl1
```
**show access-lists**

The **show access-lists** Privileged EXEC mode command displays access control lists (ACLs) defined on the device.

**Syntax**

`show access-lists [name]`

**Parameters**

- `name` — Name of the ACL.

**Default Setting**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command displays access lists on a device.

```
Console# show access-lists
IP access list ACL1
  permit ip host 172.30.40.1 any
  permit rsvp host 172.30.8.8 any
```
Address Table Commands

bridge address

The bridge address Interface Configuration (VLAN) mode command adds a MAC-layer station source address to the bridge table. To delete the MAC address, use the no form of this command.

Syntax

bridge address mac-address { ethernet interface | port-channel port-channel-number } [ permanent | delete-on-reset | delete-on-timeout | secure ]
no bridge address [ mac-address ]

Parameters

- **mac-address** — A valid MAC address.
- **interface** — A valid Ethernet port.
- **port-channel-number** — A valid port-channel number.
- **permanent** — The address can only be deleted by the no bridge address command.
- **delete-on-reset** — The address is deleted after reset.
- **delete-on-timeout** — The address is deleted after “age out” time has expired.
- **secure** — The address is deleted after the port changes mode to unlock learning (no port security command). This parameter is only available when the port is in the learning locked mode.

Default Setting

No static addresses are defined. The default mode for an added address is **permanent**.

Command Mode

Interface Configuration (VLAN) mode

Command Usage

Using the no form of the command without specifying a MAC address deletes all static MAC addresses belonging to this VLAN).

On interfaces that have an IP address configured, use the command “port security routed secure address” to configure an address with “secure” option.
Example

The following command adds a permanent static MAC-layer station source address 3aa2.64b3.a245 on port 1/e16 to the bridge table.

```
Console(config)# interface vlan 2
Console(config-if)# bridge address 3aa2.64b3.a245 ethernet 1/e16 permanent
```
**bridge multicast filtering**

The *bridge multicast filtering* Global Configuration mode command enables filtering multicast addresses. To disable filtering multicast addresses, use the **no** form of this command.

**Syntax**

`bridge multicast filtering`

`no bridge multicast filtering`

**Parameters**

There are no parameters for this command.

**Default Setting**

Filtering multicast addresses is disabled. All multicast addresses are flooded to all ports.

**Command Mode**

Global Configuration mode

**Command Usage**

If multicast devices exist on the VLAN, do not change the unregistered multicast addresses state to drop on the switch ports.

If multicast devices exist on the VLAN and IGMP-snooping is not enabled, the *bridge multicast forward-all* command should be used to enable forwarding all multicast packets to the multicast switches.

**Example**

The following command enables bridge multicast filtering.

```
Console(config)# bridge multicast filtering
```
**bridge multicast address**

The **bridge multicast address** Interface Configuration (VLAN) mode command registers a MAC-layer multicast address in the bridge table and statically adds ports to the group. To unregister the MAC address, use the **no** form of this command.

**Syntax**

```
bridge multicast address {mac-multicast-address | ip-multicast-address}
```

```
bridge multicast address {mac-multicast-address | ip-multicast-address} [add | remove]
{ethernet interface-list | port-channel port-channel-number-list}
```

```
no bridge multicast address {mac-multicast-address | ip-multicast-address}
```

**Parameters**

- **add** — Adds ports to the group. If no option is specified, this is the default option.
- **remove** — Removes ports from the group.
- **mac-multicast-address** — A valid MAC multicast address.
- **ip-multicast-address** — A valid IP multicast address.
- **interface-list** — Separate nonconsecutive Ethernet ports with a comma and no spaces; a hyphen is used to designate a range of ports.
- **port-channel-number-list** — Separate nonconsecutive port-channels with a comma and no spaces; a hyphen is used to designate a range of ports.

**Default Setting**

No multicast addresses are defined.

**Command Mode**

Interface configuration (VLAN) mode

**Command Usage**

If the command is executed without **add** or **remove**, the command only registers the group in the bridge database.

Static multicast addresses can only be defined on static VLANs.

**Examples**

The following command registers the MAC address:

```
Console(config)# interface vlan 8
Console(config-if)# bridge multicast address 01:00:5e:02:02:03
```

The following command registers the MAC address and adds ports statically.

```
Console(config)# interface vlan 8
Console(config-if)# bridge multicast address 01:00:5e:02:02:03 add ethernet 1/e1-e9,2/e2
```
bridge multicast forbidden address

The **bridge multicast forbidden address** Interface Configuration (VLAN) mode command forbids adding a specific multicast address to specific ports. Use the **no** form of this command to return to the default configuration.

**Syntax**

```
bridge multicast forbidden address {mac-multicast-address | ip-multicast-address} {add | remove} {ethernet interface-list | port-channel port-channel-number-list}
no bridge multicast forbidden address {mac-multicast-address | ip-multicast-address}
```

**Parameters**

- **add** — Defines the port as forbidden. Forbidden ports are not included in the Multicast group, even if IGMP snooping designated the port to join a Multicast group.
- **remove** — Removes ports from the Forbidden Port list.
- **mac-multicast-address** — A valid MAC multicast address.
- **ip-multicast-address** — A valid IP multicast address.
- **interface-list** — Separate nonconsecutive Ethernet ports with a comma and no spaces; hyphen is used to designate a range of ports.
- **port-channel-number-list** — Separate nonconsecutive valid port-channels with a comma and no spaces; a hyphen is used to designate a range of port-channels.

**Default Setting**

No forbidden addresses are defined.

**Command Modes**

Interface Configuration (VLAN) mode

**Command Usage**

Before defining forbidden ports, the multicast group should be registered.

**Example**

The following command forbids MAC address 0100.5e02.0203 on port 2/e9 within VLAN 8.

```
Console(config)# interface vlan 8
Console(config-if)# bridge multicast address 0100.5e02.0203
Console(config-if)# bridge multicast forbidden address 0100.5e02.0203 add ethernet 2/e9
```
**bridge multicast forward-all**

The `bridge multicast forward-all` Interface Configuration (VLAN) mode command enables forwarding all multicast packets on a port. To restore the default configuration, use the `no` form of this command.

**Syntax**

```
bridge multicast forward-all {add | remove} {ethernet interface-list | port-channel port-channel-number-list}
no bridge multicast forward-all
```

**Parameters**

- **add** — Force forwarding all multicast packets.
- **remove** — Do not force forwarding all multicast packets.
- **interface-list** — Separate nonconsecutive Ethernet ports with a comma and no spaces; a hyphen is used to designate a range of ports.
- **port-channel-number-list** — Separate nonconsecutive port-channels with a comma and no spaces; a hyphen is used to designate a range of port-channels.

**Default Setting**

This setting is disabled.

**Command Mode**

Interface Configuration (VLAN) mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command configures the device to forward all multicast packets on port 1/e8.

```
Console(config)# interface vlan 2
Console(config-if)# bridge multicast forward-all add ethernet 1/e8
```
bridge multicast forbidden forward-all

The bridge multicast forbidden forward-all Interface Configuration (VLAN) mode command forbids a port to be a forward-all-multicast port. To restore the default configuration, use the no form of this command.

Syntax

bridge multicast forbidden forward-all {add | remove} {ethernet interface-list | port-channel port-channel-number-list}

no bridge multicast forbidden forward-all

Parameters

- add — Forbids forwarding all multicast packets.
- remove — Does not forbid forwarding all multicast packets.
- interface-list — Separates nonconsecutive Ethernet ports with a comma and no spaces; a hyphen is used to designate a range of ports.
- port-channel-number-list — Separates nonconsecutive port-channels with a comma and no spaces; a hyphen is used to designate a range of port-channels.

Default Setting

This setting is disabled.

Command Mode

Interface Configuration (VLAN) mode

Command Usage

IGMP snooping dynamically discovers multicast device ports. When a multicast device port is discovered, all the multicast packets are forwarded to it unconditionally.

This command prevents a port from becoming a multicast device port.

Example

The following command configures the device to forbid all forwarding of Multicast packets to 1/e1 with VLAN 2.

```
Console(config)# interface vlan 2
Console(config-if)# bridge multicast forbidden forward-all add ethernet 1/e1
```
bridge aging-time

The **bridge aging-time** Global Configuration mode command sets the address table aging time. To restore the default configuration, use the **no** form of this command.

**Syntax**

```
bridge aging-time seconds
no bridge aging-time
```

**Parameters**

- `seconds` — Time in seconds. (Range: 10-630 seconds)

**Default Setting**

The default is 300 seconds.

**Command Mode**

Global Configuration mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command sets the bridge aging time to 250 seconds.

```
Console(config)# bridge aging-time 250
```
clear bridge

The *clear bridge* Privileged EXEC mode command removes any learned entries from the forwarding database.

**Syntax**

clear bridge

**Parameters**

There are no parameters for this command.

**Default Setting**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command clears the bridge tables.

```
Console# clear bridge
```
**port security**

The *port security* Interface Configuration mode command locks the port, thereby, blocking unknown traffic and preventing the port from learning new addresses. To return to the default configuration, use the **no** form of this command.

**Syntax**

```text
port security [forward | discard | discard-shutdown] [trap seconds]
no port security
```

**Parameters**

- **forward** — Forwards packets with unlearned source addresses, but does not learn the address.
- **discard** — Discards packets with unlearned source addresses. This is the default if no option is indicated.
- **discard-shutdown** — Discards packets with unlearned source addresses. The port is also shut down.
- **seconds** — Sends SNMP traps and defines the minimum amount of time in seconds between consecutive traps. (Range: 1-1000000)

**Default Setting**

This setting is disabled.

**Command Mode**

Interface Configuration (Ethernet, port-channel) mode

**Command Usage**

There are no user guidelines for this command.

**Example**

In the following example, port 1/e1 forwards all packets without learning addresses of packets from unknown sources and sends traps every 100 seconds if a packet with an unknown source address is received.

```text
Console(config)# interface ethernet 1/e1
Console(config-if)# port security forward trap 100
```
**port security mode**

The **port security mode** Interface Configuration mode command configures the port security mode. To return to the default configuration, use the **no** form of this command.

**Syntax**

```
port security mode {lock | dynamic}
no port security mode
```

**Parameters**

- **lock** — Saves the current dynamic MAC addresses associated with the port and disables learning, relearning and aging.
- **dynamic** — Deletes the current dynamic MAC addresses associated with the port and learns up to the maximum number addresses allowed on the port. Relearning and aging are enabled.

**Default Setting**

This setting is disabled.

**Command Mode**

Interface Configuration (Ethernet, port-channel) mode

**Command Usage**

There are no user guidelines for this command.

**Example**

In the following command, the port security mode is set to dynamic for Ethernet interface 1/e7.

```
Console(config)# interface ethernet 1/e7
Console(config-if)# port security mode dynamic
```
Address Table Commands

**port security max**

The **port security max** Interface Configuration (Ethernet, port-channel) mode command configures the maximum number of addresses that can be learned on the port while the port is in port security mode. To return to the default configuration, use the **no** form of this command.

**Syntax**

```
port security max max-addr
no port security max
```

**Parameters**

- **max-addr** — Maximum number of addresses that can be learned by the port. (Range: 1-128)

**Default Setting**

The default is 1 address.

**Command Mode**

Interface Configuration (Ethernet, port-channel) mode

**Command Usage**

This command is only relevant in dynamic learning modes.

**Example**

The following command sets the maximum number of addresses that are learned on port 1/e7 before it is locked to 20.

```
Console(config)# interface ethernet 1/e7
Console(config-if)# port security mode dynamic
Console(config-if)# port security max 20
```
**port security routed secure-address**

The **port security routed secure-address** Interface Configuration (Ethernet, port-channel) mode command adds a MAC-layer secure address to a routed port. Use the **no** form of this command to delete a MAC address.

**Syntax**

```
port security routed secure-address mac-address
no port security routed secure-address mac-address
```

**Parameters**

- `mac-address` — A valid MAC address.

**Default Setting**

No addresses are defined.

**Command Mode**

Interface Configuration (Ethernet, port-channel) mode. Cannot be configured for a range of interfaces (range context).

**Command Usage**

The command enables adding secure MAC addresses to a routed port in port security mode. The command is available when the port is a routed port and in port security mode. The address is deleted if the port exits the security mode or is not a routed port.

Use this command on interfaces that have an IP address configured, instead of the command `bridge address mac-address {ethernet interface port-channel port-channel-number} [secure].`

**Example**


```
Console(config)# interface ethernet 1/e1
```
show bridge address-table

The show bridge address-table Privileged EXEC mode command displays all entries in the bridge-forwarding database.

Syntax

show bridge address-table [vlan vlan] [ethernet interface | port-channel port-channel-number]

Parameters

- vlan — Specifies a valid VLAN, such as VLAN 1.
- interface — A valid Ethernet port.
- port-channel-number — A valid port-channel number.

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

Internal usage VLANs (VLANs that are automatically allocated on ports with a defined Layer 3 interface) are presented in the VLAN column by a port number and not by a VLAN ID.

“Special” MAC addresses that were not statically defined or dynamically learned are displayed in the MAC address table. This includes, for example, MAC addresses defined in ACLs.

Example

The following command displays all classes of entries in the bridge-forwarding database.

```
Console# show bridge address-table

Aging time is 300 sec

<table>
<thead>
<tr>
<th>Interface</th>
<th>MAC Address</th>
<th>Port</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>00:60:70:4C:73:FF</td>
<td>5/e8</td>
<td>dynamic</td>
</tr>
<tr>
<td>1</td>
<td>00:60:70:8C:73:FF</td>
<td>5/e8</td>
<td>dynamic</td>
</tr>
<tr>
<td>200</td>
<td>00:10:00:48:37:FF</td>
<td>5/e9</td>
<td>static</td>
</tr>
</tbody>
</table>
```
show bridge address-table static

The **show bridge address-table static** Privileged EXEC mode command displays statically created entries in the bridge-forwarding database.

**Syntax**

```
show bridge address-table static [vlan vlan] [ethernet interface | port-channel port-channel-number]
```

**Parameters**

- **vlan** — Specifies a valid VLAN, such as VLAN 1.
- **interface** — A valid Ethernet port.
- **port-channel-number** — A valid port-channel number.

**Default Setting**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command displays all static entries in the bridge-forwarding database.

```
Console# show bridge address-table static

Aging time is 300 sec

<table>
<thead>
<tr>
<th>VLAN</th>
<th>MAC Address</th>
<th>Port</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>----</td>
<td>------------------</td>
<td>------</td>
<td>------------------</td>
</tr>
<tr>
<td>1</td>
<td>00:60:70:4C:73:FF</td>
<td>1/e8</td>
<td>Permanent</td>
</tr>
<tr>
<td>1</td>
<td>00:60.70.8C:73:FF</td>
<td>1/e8</td>
<td>delete-on-timeout</td>
</tr>
<tr>
<td>200</td>
<td>00:10:0D:48:37:FF</td>
<td>1/e9</td>
<td>delete-on-reset</td>
</tr>
</tbody>
</table>
```
**show bridge address-table count**

The *show bridge address-table count* Privileged EXEC mode command displays the number of addresses present in the Forwarding Database.

**Syntax**

```
show bridge address-table count [vlan vlan][ ethernet interface-number ]| port-channel port-channel-number
```

**Parameters**

- `vlan` — Specifies a valid VLAN, such as VLAN 1.
- `interface` — A valid Ethernet port.
- `port-channel-number` — A valid port-channel number.

**Default Setting**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command displays the number of addresses present in all VLANs.

```
Console# show bridge address-table count

Capacity: 8192  
Free: 8083  
Used: 109

Secure addresses: 2  
Static addresses: 1  
Dynamic addresses: 97  
Internal addresses: 9
```
**show bridge multicast address-table**

The `show bridge multicast address-table` User EXEC mode command displays multicast MAC address or IP address table information.

**Syntax**

```
show bridge multicast address-table [vlan vlan-id] [address mac-multicast-address | ip-multicast-address] [format ip | format mac]
```

**Parameters**

- `vlan vlan-id` — A valid VLAN ID value.
- `mac-multicast-address` — A valid MAC multicast address.
- `ip-multicast-address` — A valid IP multicast address.
- `format ip | mac` — Multicast address format. Can be `ip` or `mac`. If the format is unspecified, the default is `mac`.

**Default Setting**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode

**Command Usage**

A MAC address can be displayed in IP format only if it is in the range of 0100.5e00.0000-0100.5e7f.ffff.

**Example**

The following command displays Multicast MAC address and IP address table information.

```
Console# show bridge multicast address-table

<table>
<thead>
<tr>
<th>VLAN</th>
<th>MAC Address</th>
<th>Type</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>01:00:5e:02:02:03</td>
<td>static</td>
<td>1/e1, 2/e2</td>
</tr>
<tr>
<td>19</td>
<td>01:00:5e:02:02:08</td>
<td>static</td>
<td>1/e1-e8</td>
</tr>
<tr>
<td>19</td>
<td>00:00:5e:02:02:08</td>
<td>dynamic</td>
<td>1/e9-e11</td>
</tr>
</tbody>
</table>

Forbidden ports for multicast addresses:

<table>
<thead>
<tr>
<th>VLAN</th>
<th>MAC Address</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>01:00:5e:02:02:03</td>
<td>2/e8</td>
</tr>
<tr>
<td>19</td>
<td>01:00:5e:02:02:08</td>
<td>2/e8</td>
</tr>
</tbody>
</table>
```
A multicast MAC address maps to multiple IP addresses as shown in the example.

```
Console# show bridge multicast address-table format ip

<table>
<thead>
<tr>
<th>VLAN</th>
<th>IP/MAC Address</th>
<th>Type</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>224-239.130/2.2.3</td>
<td>static</td>
<td>1/e1,2/e2</td>
</tr>
<tr>
<td>19</td>
<td>224-239.130/2.2.8</td>
<td>static</td>
<td>1/e1-8</td>
</tr>
<tr>
<td>19</td>
<td>224-239.130/2.2.8</td>
<td>dynamic</td>
<td>1/e9-11</td>
</tr>
</tbody>
</table>

Forbidden ports for multicast addresses:

<table>
<thead>
<tr>
<th>VLAN</th>
<th>IP/MAC Address</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>224-239.130/2.2.3</td>
<td>2/e8</td>
</tr>
<tr>
<td>19</td>
<td>224-239.130/2.2.8</td>
<td>2/e8</td>
</tr>
</tbody>
</table>
```
show bridge multicast filtering

The show bridge multicast filtering User EXEC mode command displays the multicast filtering configuration.

Syntax
show bridge multicast filtering vlan-id

Parameters
- vlan-id — VLAN ID value.

Default Setting
This command has no default configuration.

Command Mode
User EXEC mode

Command Usage
There are no user guidelines for this command.

Example
The following command displays the Multicast configuration for VLAN 1.

```
Console# show bridge multicast filtering 1

Filtering: Enabled
VLAN: 1

<table>
<thead>
<tr>
<th>Port</th>
<th>Forward-Unregistered</th>
<th>Forward-All</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Static</td>
<td>Status</td>
</tr>
<tr>
<td>----</td>
<td>--------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>1/e1</td>
<td>Forbidden</td>
<td>Filter</td>
</tr>
<tr>
<td>1/e2</td>
<td>Forward</td>
<td>Forward(s)</td>
</tr>
<tr>
<td>1/e3</td>
<td>-</td>
<td>Forward(d)</td>
</tr>
</tbody>
</table>
```
show ports security

The show ports security Privileged EXEC mode command displays the port-lock status.

Syntax

show ports security [ethernet interface | port-channel port-channel-number]

Parameters

- interface — A valid Ethernet port.
- port-channel-number — A valid port-channel number.

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following command displays all classes of port-lock status entries.

```
Console# show ports security
```

<table>
<thead>
<tr>
<th>Port</th>
<th>Status</th>
<th>Learning</th>
<th>Action</th>
<th>Maximum</th>
<th>Trap</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/e1</td>
<td>Locked</td>
<td>Dynamic</td>
<td>Discard</td>
<td>3</td>
<td>Enable</td>
<td>100</td>
</tr>
<tr>
<td>1/e2</td>
<td>Unlocked</td>
<td>Dynamic</td>
<td>-</td>
<td>28</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>1/e3</td>
<td>Locked</td>
<td>Disabled</td>
<td>Discard, Shutdown</td>
<td>8</td>
<td>Disable</td>
<td>-</td>
</tr>
</tbody>
</table>

The following table describes the fields shown in the example.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Port number</td>
</tr>
<tr>
<td>Status</td>
<td>Locked/Unlocked</td>
</tr>
<tr>
<td>Learning</td>
<td>Learning mode</td>
</tr>
<tr>
<td>Action</td>
<td>Action on violation</td>
</tr>
<tr>
<td>Maximum</td>
<td>Maximum addresses that can be associated on this port in Static Learning mode or in Dynamic Learning mode</td>
</tr>
<tr>
<td>Trap</td>
<td>Indicates if traps are sent in case of a violation</td>
</tr>
<tr>
<td>Frequency</td>
<td>Minimum time between consecutive trap</td>
</tr>
</tbody>
</table>
show ports security addresses

The `show ports security addresses` Privileged EXEC mode command displays the current dynamic addresses in locked ports.

**Syntax**

`show ports security addresses [ethernet interface | port-channel port-channel-number]`

**Parameters**

- `interface` — A valid Ethernet port.
- `port-channel-number` — A valid port-channel number

**Default Setting**

This command has no default configuration.

**Command Mode**

Privileged EXEC Mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command displays the dynamic addresses in currently locked ports.

```console
Console# show ports security addresses

<table>
<thead>
<tr>
<th>Port</th>
<th>Status</th>
<th>Learning</th>
<th>Current</th>
<th>Maximum</th>
</tr>
</thead>
<tbody>
<tr>
<td>----</td>
<td>------------</td>
<td>----------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>1/e1</td>
<td>Disabled</td>
<td>Lock</td>
<td>-</td>
<td>1</td>
</tr>
<tr>
<td>1/e2</td>
<td>Disabled</td>
<td>Lock</td>
<td>-</td>
<td>1</td>
</tr>
<tr>
<td>1/e3</td>
<td>Enabled</td>
<td>Max-addresses</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1/e4</td>
<td>Port is a member in port-channel ch1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1/e5</td>
<td>Disabled</td>
<td>Lock</td>
<td>-</td>
<td>1</td>
</tr>
<tr>
<td>1/e6</td>
<td>Enabled</td>
<td>Max-addresses</td>
<td>0</td>
<td>10</td>
</tr>
<tr>
<td>ch1</td>
<td>Enabled</td>
<td>Max-addresses</td>
<td>0</td>
<td>50</td>
</tr>
<tr>
<td>ch2</td>
<td>Enabled</td>
<td>Max-addresses</td>
<td>0</td>
<td>128</td>
</tr>
</tbody>
</table>
```

The following command displays the dynamic addresses in currently locked port 1/e1.

```console
Console# show ports security addresses ethernet 1/e1

<table>
<thead>
<tr>
<th>Port</th>
<th>Status</th>
<th>Learning</th>
<th>Current</th>
<th>Maximum</th>
</tr>
</thead>
<tbody>
<tr>
<td>----</td>
<td>------------</td>
<td>----------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>1/e1</td>
<td>Disabled</td>
<td>Lock</td>
<td>-</td>
<td>1</td>
</tr>
</tbody>
</table>
```
clock set

The clock set Privileged EXEC mode command manually sets the system clock.

Syntax

clock set hh:mm:ss day month year

or

clock set hh:mm:ss month day year

Parameters

■ hh:mm:ss — Current time in hours (military format), minutes, and seconds (hh: 0-23, mm: 0-59, ss: 0-59).

■ day — Current day (by date) in the month (1-31).

■ month — Current month using the first three letters by name (Jan, …, Dec).


Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following command sets the system time to 13:32:00 on March 7th, 2006.

```
Console# clock set 13:32:00 7 Mar 2006
```
clock source

The **clock source** Global Configuration mode command configures an external time source for the system clock. Use **no** form of this command to disable external time source.

**Syntax**
clock source {sntp}
no clock source

**Parameters**
- **sntp** — SNTP servers

**Default Setting**
No external clock source.

**Command Mode**
Global Configuration mode

**Command Usage**
There are no user guidelines for this command.

**Example**
The following command configures an external time source for the system clock.

```
Console(config)# clock source sntp
```
**clock timezone**

The **clock timezone** Global Configuration mode command sets the time zone for display purposes. To set the time to the Coordinated Universal Time (UTC), use the **no** form of this command.

**Syntax**

```
clock timezone hours-offset [minutes minutes-offset] [zone acronym]
no clock timezone
```

**Parameters**

- **hours-offset** — Hours difference from UTC. (Range: -12 – +13)
- **minutes-offset** — Minutes difference from UTC. (Range: 0–59 minutes)
- **acronym** — The acronym of the time zone. (Range: Up to 4 characters)

**Default Setting**

Clock set to UTC.

**Command Mode**

Global Configuration mode

**Command Usage**

The system internally keeps time in UTC, so this command is used only for display purposes and when the time is manually set.

**Example**

The following command sets the time zone to 6 hours difference from UTC.

```
Console(config)# clock timezone -6 zone CST
```
clock summer-time

The **clock summer-time** Global Configuration mode command configures the system to automatically switch to summer time (daylight saving time). To configure the software not to automatically switch to summer time, use the **no** form of this command.

**Syntax**

```
clock summer-time recurring {usa | eu | {week day month hh:mm week day month hh:mm}}
[offset offset] [zone acronym]
clock summer-time date date month year hh:mm date month year hh:mm [offset offset] [zone acronym]
clock summer-time date month date year hh:mm month date year hh:mm [offset offset] [zone acronym]
```

**Parameters**

- **recurring** — Indicates that summer time should start and end on the corresponding specified days every year.
- **date** — Indicates that summer time should start on the first specific date listed in the command and end on the second specific date in the command.
- **usa** — The summer time rules are the United States rules.
- **eu** — The summer time rules are the European Union rules.
- **week** — Week of the month. (Range: 1-5, **first**, **last**)
- **day** — Day of the week (Range: first three letters by name, like **sun**)
- **date** — Date of the month. (Range:1-31)
- **month** — Month. (Range: first three letters by name, like Jan)
- **year** — year - no abbreviation (Range: 2000-2097)
- **hh:mm** — Time in military format, in hours and minutes. (Range: hh: 0-23, mm: 0-59)
- **offset** — Number of minutes to add during summer time. (Range: 1-1440)
- **acronym** — The acronym of the time zone to be displayed when summer time is in effect. (Range: Up to 4 characters)

**Default Setting**

- Summer time is disabled by default.
- **offset** — Default summer time is 60 minutes.
- **acronym** — If unspecified default to the timezone acronym.
- If the time zone has not been defined, the default is UTC.

**Command Mode**

Global Configuration mode
**Command Usage**

In both the **date** and **recurring** forms of the command, the first part of the command specifies when summer time begins, and the second part specifies when it ends. All times are relative to the local time zone. The start time is relative to standard time. The end time is relative to summer time. If the starting month is chronologically after the ending month, the system assumes that the user is in the southern hemisphere.

USA rule for daylight savings time:
- Start: First Sunday in April
- End: Last Sunday in October
- Time: 2 am local time

EU rule for daylight savings time:
- Start: Last Sunday in March
- End: Last Sunday in October
- Time: 1.00 am (01:00)

**Example**

The following command sets the summer time, starting on the first Sunday in April at 2 am and finishing on the last Sunday in October at 2 am.

```
Console(config)# clock summer-time recurring first sun apr 2:00 last sun oct 2:00
```
sntp authentication-key

The `sntp authentication-key` Global Configuration mode command defines an authentication key for Simple Network Time Protocol (SNTP). To remove the authentication key for SNTP, use the `no` form of this command.

**Syntax**

```
sntp authentication-key number md5 value
no sntp authentication-key number
```

**Parameters**

- `number` — Key number (Range: 1-4294967295)
- `value` — Key value (Range: 1-8 characters)

**Default Setting**

No authentication key is defined.

**Command Mode**

Global Configuration mode

**Command Usage**

Multiple keys can be generated.

**Example**

The following command defines the authentication key for SNTP.

```
Console(config)# sntp authentication-key 8 md5 ClkKey
```
**sntp authenticate**

The `sntp authenticate` Global Configuration mode command grants authentication for received Simple Network Time Protocol (SNTP) traffic from servers. To disable the feature, use the `no` form of this command.

**Syntax**
```
sntp authenticate
no sntp authenticate
```

**Parameters**
There are no parameters for this command.

**Default Setting**
No authentication

**Command Mode**
Global Configuration mode

**Command Usage**
The command is relevant for both unicast and broadcast.

**Example**
The following command defines the authentication key for SNTP and grants authentication.

```
Console(config)# sntp authentication-key 8 md5 ClkKey
Console(config)# sntp trusted-key 8
Console(config)# sntp authenticate
```
**sntp trusted-key**

The `sntp trusted-key` Global Configuration mode command authenticates the identity of a system to which Simple Network Time Protocol (SNTP) will synchronize. To disable authentication of the identity of the system, use the `no` form of this command.

**Syntax**

`sntp trusted-key key-number`

`no sntp trusted-key key-number`

**Parameters**

- `key-number` — Key number of authentication key to be trusted. (Range: 1-4294967295)

**Default Setting**

No keys are trusted.

**Command Mode**

Global Configuration mode

**Command Usage**

The command is relevant for both received unicast and broadcast.

If there is at least 1 trusted key, then unauthenticated messages will be ignored.

**Example**

The following command authenticates key number 8.

```
Console(config)# sntp authentication-key 8 md5 ClkKey
Console(config)# sntp trusted-key 8
Console(config)# sntp authenticate
```
**sntp client poll timer**

The `sntp client poll timer` Global Configuration mode command sets the polling time for the Simple Network Time Protocol (SNTP) client. To return to default configuration, use the `no` form of this command.

**Syntax**

```
sntp client poll timer seconds
no sntp client poll timer
```

**Parameters**

- `seconds` — Polling interval in seconds (Range: 60-86400)

**Default Setting**

Polling interval is 1024 seconds.

**Command Mode**

Global Configuration mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command sets the polling time for the Simple Network Time Protocol (SNTP) client to 120 seconds.

```
Console(config)# sntp client poll timer 120
```
sntp broadcast client enable

The `sntp broadcast client enable` Global Configuration mode command enables Simple Network Time Protocol (SNTP) broadcast clients. To disable SNTP broadcast clients, use the `no` form of this command.

**Syntax**

```
sntp broadcast client enable
no sntp broadcast client enable
```

**Parameters**

There are no parameters for this command.

**Default Setting**

The SNTP broadcast client is disabled.

**Command Mode**

Global Configuration mode

**Command Usage**

Use the `sntp client enable (Interface)` Interface Configuration mode command to enable the SNTP client on a specific interface.

**Example**

The following command enables the SNTP broadcast clients.

```
Console(config)# sntp broadcast client enable
```
**sntp anycast client enable**

The **sntp anycast client enable** Global Configuration mode command enables SNTP anycast client. To disable the SNTP anycast client, use the **no** form of this command.

**Syntax**

```
sntp anycast client enable
no sntp anycast client enable
```

**Parameters**

There are no parameters for this command.

**Default Setting**

The SNTP anycast client is disabled.

**Command Mode**

Global Configuration mode

**Command Usage**

Polling time is determined by the **sntp client poll timer** Global Configuration mode command.

Use the **sntp client enable (Interface)** Interface Configuration mode command to enable the SNTP client on a specific interface.

**Example**

The following command enables the SNTP anycast clients.

```
Console(config)# sntp anycast client enable
```
**sntp client enable (Interface)**

The `sntp client enable` Interface Configuration (Ethernet, port-channel, VLAN) mode command enables the Simple Network Time Protocol (SNTP) client on an interface. This applies to both receive broadcast and anycast updates. To disable the SNTP client, use the `no` form of this command.

**Syntax**

```
sntp client enable
no sntp client enable
```

**Parameters**

There are no parameters for this command.

**Default Setting**

The SNTP client is disabled on an interface.

**Command Mode**

Interface configuration (Ethernet, port-channel, VLAN) mode

**Command Usage**

Use the `sntp broadcast client enable` Global Configuration mode command to enable broadcast clients globally.

Use the `sntp anycast client enable` Global Configuration mode command to enable anycast clients globally.

**Example**

The following command enables the SNTP client on Ethernet port 1/e3.

```
Console(config)# interface ethernet 1/e3
Console(config-if)# sntp client enable
```
**sntp unicast client enable**

The `sntp unicast client enable` Global Configuration mode command enables the device to use the Simple Network Time Protocol (SNTP) to request and accept SNTP traffic from servers. To disable requesting and accepting SNTP traffic from servers, use the `no` form of this command.

**Syntax**

- `sntp unicast client enable`
- `no sntp unicast client enable`

**Parameters**

There are no parameters for this command.

**Default Setting**

The SNTP unicast client is disabled.

**Command Mode**

Global Configuration mode

**Command Usage**

Use the `sntp server` Global Configuration mode command to define SNTP servers.

**Example**

The following command enables the device to use the Simple Network Time Protocol (SNTP) to request and accept SNTP traffic from servers.

```plaintext
Console(config)# sntp unicast client enable
```
Clock Commands

**sntp unicast client poll**

The **sntp unicast client poll** Global Configuration mode command enables polling for the Simple Network Time Protocol (SNTP) predefined unicast servers. To disable the polling for SNTP client, use the **no** form of this command.

**Syntax**

```
sntp unicast client poll
no sntp unicast client poll
```

**Parameters**

There are no parameters for this command.

**Default Setting**

Polling is disabled.

**Command Mode**

Global Configuration mode

**Command Usage**

Polling time is determined by the **sntp client poll timer** Global Configuration mode command.

**Example**

The following command enables polling for SNTP predefined unicast clients.

```
Console(config)# sntp unicast client poll
```
sntp server

The sntp server Global Configuration mode command configures the device to use the Simple Network Time Protocol (SNTP) to request and accept SNTP traffic from a specified server. To remove a server from the list of SNTP servers, use the no form of this command.

Syntax

sntp server {ip-address | hostname}[poll] [key keyid]

no sntp server host

Parameters

- **ip-address** — IP address of the server.
- **hostname** — Hostname of the server. (Range: 1-158 characters)
- **poll** — Enable polling.
- **keyid** — Authentication key to use when sending packets to this peer.
  (Range: 1-4294967295)

Default Setting

No servers are defined.

Command Mode

Global Configuration mode

Command Usage

Up to 8 SNTP servers can be defined.

Use the sntp unicast client enable Global Configuration mode command to enable predefined unicast clients globally.

To enable polling you should also use the sntp unicast client poll Global Configuration mode command for global enabling.

Polling time is determined by the sntp client poll timer Global Configuration mode command.

Example

The following command configures the device to accept SNTP traffic from the server on 192.1.1.1.

```
Console(config)# sntp server 192.1.1.1
```
show clock

The **show clock** User EXEC mode command displays the time and date from the system clock.

**Syntax**

```text
show clock [detail]
```

**Parameters**

- **detail** — Shows timezone and summertime configuration.

**Default Setting**

This command has no default configuration.

**Command Mode**

User EXEC mode

**Command Usage**

The symbol that precedes the show clock display indicates the following information:

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Time is not authoritative.</td>
</tr>
<tr>
<td>(blank)</td>
<td>Time is authoritative.</td>
</tr>
<tr>
<td>.</td>
<td>Time is authoritative, but SNTP is not synchronized.</td>
</tr>
</tbody>
</table>

**Example**

The following command displays the time and date from the system clock.

```
Console> show clock
15:29:03 PDT(UTC-7) Jun 17 2006
Time source is SNTP

Console> show clock detail
15:29:03 PDT(UTC-7) Jun 17 2006
Time source is SNTP
Time zone:
  Acronym is PST
  Offset is UTC-8
Summertime:
  Acronym is PDT
  Recurring every year.
  Begins at first Sunday of April at 2:00.
  Ends at last Sunday of October at 2:00.
  Offset is 60 minutes.
```
**show sntp configuration**

The **show sntp configuration** Privileged EXEC mode command shows the configuration of the Simple Network Time Protocol (SNTP).

**Syntax**

```
show sntp configuration
```

**Parameters**

There are no parameters for this command.

**Default Setting**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command displays the current SNTP configuration of the device.

```
Console# show sntp configuration

Polling interval: 7200 seconds

MD5 Authentication keys: 8, 9
Authentication is required for synchronization.
Trusted Keys: 8, 9

Unicast Clients: Enabled
Unicast Clients Polling: Enabled

<table>
<thead>
<tr>
<th>Server</th>
<th>Polling</th>
<th>Encryption Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>176.1.1.8</td>
<td>Enabled</td>
<td>9</td>
</tr>
<tr>
<td>176.1.8.179</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

Broadcast Clients: Enabled
Anycast Clients: Enabled
Broadcast and Anycast Interfaces: 1/e1, 1/e3
show sntp status

The `show sntp status` Privileged EXEC mode command shows the status of the Simple Network Time Protocol (SNTP).

**Syntax**

```
show sntp status
```

**Parameters**

There are no parameters for this command.

**Default Setting**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command shows the status of the SNTP.

```
Console# show sntp status
Clock is synchronized, stratum 4, reference is 176.1.1.8, unicast
Reference time is AFE2525E.70597B34 (00:10:22.438 PDT Jul 5 2006)

Unicast servers:

<table>
<thead>
<tr>
<th>Server</th>
<th>Status</th>
<th>Last Response</th>
<th>Offset [mSec]</th>
<th>Delay [mSec]</th>
</tr>
</thead>
<tbody>
<tr>
<td>176.1.1.8</td>
<td>Up</td>
<td>19:58:22.289 PDT Feb 19 2006</td>
<td>7.33</td>
<td>117.79</td>
</tr>
<tr>
<td>176.1.8.179</td>
<td>Unknown</td>
<td>12:17:17.987 PDT Feb 19 2006</td>
<td>8.98</td>
<td>189.19</td>
</tr>
</tbody>
</table>

Anycast Server:

<table>
<thead>
<tr>
<th>Server</th>
<th>Interface</th>
<th>Status</th>
<th>Last Response</th>
<th>Offset [mSec]</th>
<th>Delay [mSec]</th>
</tr>
</thead>
</table>

Broadcast:

<table>
<thead>
<tr>
<th>Interface</th>
<th>Interface</th>
<th>Last Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>176.9.1.1</td>
<td>VLAN 119</td>
<td>19:17:59.792 PDT Feb 19 2006</td>
</tr>
</tbody>
</table>
Configuration and Image File Commands

copy

The **copy** Privileged EXEC mode command copies files from a source to a destination.

**Syntax**

copy source-url destination-url

**Parameters**

- **source-url** — The source file location URL or reserved keyword of the source file to be copied.
  (Range: 1-160 characters)
- **destination-url** — The destination file URL or reserved keyword of the destination file.
  (Range: 1-160 characters)

The following table displays keywords and URL prefixes:

<table>
<thead>
<tr>
<th><strong>Keyword</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>flash:</td>
<td>Source or destination URL for flash memory. This is the default in case a URL is specified without a prefix.</td>
</tr>
<tr>
<td>running-config</td>
<td>Represents the current running configuration file.</td>
</tr>
<tr>
<td>startup-config</td>
<td>Represents the startup configuration file.</td>
</tr>
<tr>
<td>image</td>
<td>If the source file, represents the active image file. If the destination file, represents the non-active image file.</td>
</tr>
<tr>
<td>boot</td>
<td>Boot file.</td>
</tr>
<tr>
<td>tftp://</td>
<td>Source or destination URL for a TFTP network server. The syntax for this alias is tftp://host/[directory]/filename. The host can be represented by its IP address or hostname.</td>
</tr>
<tr>
<td>null:</td>
<td>Null destination for copies or files. A remote file can be copied to null to determine its size.</td>
</tr>
<tr>
<td>backup-config</td>
<td>Represents the backup configuration file. This is a user-defined name for up to five backup configuration files.</td>
</tr>
</tbody>
</table>

**Default Setting**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode
Configuration and Image File Commands

Command Usage

Up to five backup configuration files are supported on the device.

The location of a file system dictates the format of the source or destination URL.

The entire copying process may take several minutes and differs from protocol to protocol and from network to network.

*.prv and *.sys files cannot be copied.

Understanding Invalid Combinations of Source and Destination

Some invalid combinations of source and destination exist. Specifically, you cannot copy if one of the following conditions exist:

- The source file and destination file are the same file.
- tftp:// is the source file and destination file on the same copy.

The following table describes copy characters:

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>!</td>
<td>For network transfers, indicates that the copy process is taking place. Each exclamation point indicates successful transfer of ten packets (512 bytes each).</td>
</tr>
<tr>
<td>.</td>
<td>For network transfers, indicates that the copy process timed out. Generally, many periods in a row means that the copy process may fail.</td>
</tr>
</tbody>
</table>

Copying an Image File from a Server to Flash Memory

To copy an image file from a server to flash memory, use the `copy source-url image` command.

Copying a Boot File from a Server to Flash Memory

To copy a boot file from a server to flash memory, enter the `copy source-url boot` command.

Copying a Configuration File from a Server to the Running Configuration File

To load a configuration file from a network server to the running configuration file of the device, enter the `copy source-url running-config` command. The commands in the loaded configuration file are added to those in the running configuration file as if the commands were typed in the command-line interface (CLI). Thus, the resulting configuration file is a combination of the previous running configuration and the loaded configuration files with the loaded configuration file taking precedence.

Copying a Configuration File from a Server to the Startup Configuration

To copy a configuration file from a network server to the startup configuration file of the device, enter `copy source-url startup-config`. The startup configuration file is replaced by the copied configuration file.

Storing the Running or Startup Configuration on a Server

Use the `copy running-config destination-url` command to copy the current configuration file to a network server using TFTP. Use the `copy startup-config destination-url` command to copy the startup configuration file to a network server.

Saving the Running Configuration to the Startup Configuration

To copy the running configuration to the startup configuration file, enter the `copy running-config startup-config` command.
Backing up the Running or Startup Configuration to a Backup Configuration File

To copy the running configuration file to a backup configuration file, enter the `copy running-config file` command. To copy the startup configuration file to a backup configuration file, enter the `copy startup-config file` command.

Before copying from the backup configuration file to the running configuration file, make sure that the backup configuration file has not been corrupted.

**Example**

The following command copies system image file1 from the TFTP server 172.16.101.101 to a non-active image file.

```
Console# copy tftp://172.16.101.101/file1 image

   Accessing file 'file1' on 172.16.101.101...
   Loading file1 from 172.16.101.101: !!!!!!!!!!!!!!!!!!!!!!!!!!
      !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
      [OK]
Copy took 0:01:11 [hh:mm:ss]
```
delete

The **delete** Privileged EXEC mode command deletes a file from a flash memory device.

**Syntax**

delete url

**Parameters**

- **url** — The location URL or reserved keyword of the file to be deleted. (Range: 1-160 characters)

The following table displays keywords and URL prefixes:

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>flash</td>
<td>Source or destination URL for flash memory. This is the default when a URL is specified without a prefix.</td>
</tr>
<tr>
<td>startup-config</td>
<td>Represents the startup configuration file.</td>
</tr>
</tbody>
</table>

**Default Setting**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode

**Command Usage**

*.sys, *.prv, image-1 and image-2 files cannot be deleted.

**Example**

The following command deletes file **test** from flash memory.

```
Console# delete flash:test
Delete flash:test? [confirm]
```
**boot system**

The `boot system` Privileged EXEC mode command specifies the system image that the device loads at startup.

**Syntax**

`boot system {image-1 | image-2}`

**Parameters**

- `image-1` — Specifies image 1 as the system startup image.
- `image-2` — Specifies image 2 as the system startup image.

**Default Setting**

The command has no default configuration.

**Command Mode**

Privileged EXEC mode

**Command Usage**

Use the `show bootvar` command to find out which image is the active image.

**Example**

The following command loads system image 1 at device startup.

```
Console# boot system image-1
```
**show running-config**

The `show running-config` Privileged EXEC mode command displays the contents of the currently running configuration file.

**Syntax**

```
show running-config
```

**Parameters**

There are no parameters for this command.

**Default Setting**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command displays the contents of the running configuration file.

```
Console# show running-config
  software version 1.1
  hostname device
  interface ethernet 1/e1
    ip address 176.242.100.100 255.255.255.0
    duplex full
    speed 100
  interface ethernet 1/e2
    ip address 176.243.100.100 255.255.255.0
    duplex full
    speed 100
```
**show startup-config**

The `show startup-config` Privileged EXEC mode command displays the contents of the startup configuration file.

**Syntax**

```
show startup-config
```

**Parameters**

There are no parameters for this command.

**Default Setting**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command displays the contents of the running configuration file.

```
Console# show startup-config
  software version 1.1
  hostname device
  interface ethernet 1/e1
  ip address 176.242.100.100 255.255.255.0
  duplex full
  speed 100
  interface ethernet 1/e2
  ip address 176.243.100.100 255.255.255.0
  duplex full
  speed 100
```
**show bootvar**

The `show bootvar` Privileged EXEC mode command displays the active system image file that is loaded by the device at startup.

**Syntax**

```
show bootvar
```

**Parameters**

There are no parameters for this command.

**Default Setting**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command displays the active system image file that is loaded by the device at startup.

```
Console# show bootvar
Images currently available on the flash
image-1       active
image-2       not active (selected for next boot)

<table>
<thead>
<tr>
<th>Active Image</th>
<th>Selected for Next Boot</th>
</tr>
</thead>
<tbody>
<tr>
<td>image-1</td>
<td>image-2</td>
</tr>
<tr>
<td>image-1</td>
<td>image-1</td>
</tr>
</tbody>
</table>
```
interface ethernet

The interface ethernet Global Configuration mode command enters the interface configuration mode to configure an Ethernet type interface.

Syntax
interface ethernet interface

Parameters
- interface — Valid Ethernet port. (Full syntax: port)

Default Setting
This command has no default configuration.

Command Mode
Global Configuration mode

Command Usage
There are no user guidelines for this command.

Example
The following command enables configuring Ethernet port 5/e18.

```
Console(config)# interface ethernet 5/e18
```
interface range ethernet

The **interface range ethernet** Global Configuration mode command configures multiple Ethernet type interfaces at the same time.

**Syntax**

```
interface range ethernet {port-range | all}
```

- **port-range** — List of valid ports. Where more than one port is listed, separate nonconsecutive ports with a comma and no spaces, use a hyphen to designate a range of ports and group a list separated by commas in brackets.

- **all** — All Ethernet ports.

**Default Setting**

This command has no default configuration.

**Command Mode**

Global Configuration mode

**Command Usage**

Commands under the interface range context are executed independently on each active interface in the range. If the command returns an error on one of the active interfaces, it does not stop executing commands on other active interfaces.

**Example**

The following example shows how ports 5/e18 to 5/e20 and 3/e1 to 3/24 are grouped to receive the same command.

```
Console(config)# interface range ethernet 5/e18-5/e20/3/e1-3/e24
Console(config-if)#
```
**shutdown**

The `shutdown` Interface Configuration (Ethernet, port-channel) mode command disables an interface. To restart a disabled interface, use the `no` form of this command.

**Syntax**

`shutdown`  
`no shutdown`

**Parameters**

There are no parameters for this command.

**Default Setting**

The interface is disabled.

**Command Mode**

Interface Configuration (Ethernet, port-channel) mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command disables Ethernet port 1/e5 operations.

```
Console(config)# interface ethernet 1/e5  
Console(config-if)# shutdown
```

The following command restarts the disabled Ethernet port.

```
Console(config)# interface ethernet 1/e5  
Console(config-if)# no shutdown
```
description

The description Interface Configuration (Ethernet, port-channel) mode command adds a description to an interface. To remove the description, use the no form of this command.

Syntax

description string

no description

Parameters

■ string — Comment or a description of the port to enable the user to remember what is attached to the port. (Range: 1-64 characters)

Default Setting

The interface does not have a description.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

Command Usage

There are no user guidelines for this command.

Example

The following command adds a description to Ethernet port 1/e5.

```
Console(config)# interface ethernet 1/e5
Console(config-if)# description "RD SW#3"
```
speed

The **speed** Interface Configuration (Ethernet, port-channel) mode command configures the speed of a given Ethernet interface when not using auto-negotiation. To restore the default configuration, use the **no** form of this command.

**Syntax**

speed {10 | 100 | 1000}

no speed

**Parameters**

- **10** — Forces 10 Mbps operation.
- **100** — Forces 100 Mbps operation.
- **1000** — Forces 1000 Mbps operation.

**Default Setting**

Maximum port capability

**Command Mode**

Interface Configuration (Ethernet, port-channel) mode

**Command Usage**

The **no speed** command in a port-channel context returns each port in the port-channel to its maximum capability.

**Example**

The following command configures the speed operation of Ethernet port 1/e5 to 100 Mbps operation.

```
Console(config)# interface ethernet 1/e5
Console(config-if)# speed 100
```
duplex

The **duplex** Interface Configuration (Ethernet) mode command configures the full/half duplex operation of a given Ethernet interface when not using auto-negotiation. To restore the default configuration, use the **no** form of this command.

**Syntax**

duplex {half | full}

no duplex

**Parameters**

- **half** — Forces half-duplex operation
- **full** — Forces full-duplex operation

**Default Setting**

The interface is set to full duplex.

**Command Mode**

Interface Configuration (Ethernet) mode

**Command Usage**

When configuring a particular duplex mode on the port operating at 10/100 Mbps, disable the auto-negotiation on that port.

Half duplex mode can be set only for ports operating at 10 Mbps or 100 Mbps.

**Example**

The following command configures the duplex operation of Ethernet port 1/e5 to full duplex operation.

```
Console(config)# interface ethernet 1/e5
Console(config-if)# duplex full
```
negotiation

The **negotiation** Interface Configuration (Ethernet, port-channel) mode command enables auto-negotiation operation for the speed and duplex parameters of a given interface. To disable auto-negotiation, use the **no** form of this command.

**Syntax**

```
negotiation [capability1 [capability2…capability5]]

no negotiation
```

**Parameters**

- `capability` — Specifies the capabilities to advertise. (Possible values: 10h, 10f, 100h, 100f, 1000f)

**Default Setting**

Auto-negotiation is enabled.

If unspecified, the default setting is to enable all capabilities of the port.

**Command Mode**

Interface Configuration (Ethernet, port-channel) mode

**Command Usage**

If capabilities were specified when auto-negotiation was previously entered, not specifying capabilities when currently entering auto-negotiation overrides the previous configuration and enables all capabilities.

**Example**

The following command enables auto-negotiation on Ethernet port 1/e5.

```
Console(config)# interface ethernet 1/e5
Console(config-if)# negotiation
```
### flowcontrol

The `flowcontrol` Interface Configuration (Ethernet, port-channel) mode command configures flow control on a given interface. To disable flow control, use the `no` form of this command.

**Syntax**

```plaintext
flowcontrol {auto | on | off}
no flowcontrol
```

**Parameters**

- **auto** — Indicates auto-negotiation
- **on** — Enables flow control.
- **off** — Disables flow control.

**Default Setting**

Flow control is off.

**Command Mode**

Interface Configuration (Ethernet, port-channel) mode

**Command Usage**

Negotiation should be enabled for `flowcontrol auto`.

**Example**

In the following example, flow control is enabled on port 1/e5.

```plaintext
Console(config)# interface ethernet 1/e5
Console(config-if)# flowcontrol on
```
The **mdix** Interface Configuration (Ethernet) mode command enables cable crossover on a given interface. To disable cable crossover, use the **no** form of this command.

**Syntax**

```
mdix {on | auto}
no mdix
```

**Parameters**

- **on** — Manual mdix
- **auto** — Automatic mdi/mdix

**Default Setting**

- **auto** for ports 42-46
- **on** for port 41
- **off** for ports 1-40

**Command Mode**

Interface Configuration (Ethernet) mode

**Command Usage**

**Auto:** All possibilities to connect a PC with cross or normal cables are supported and are automatically detected.

**On:** It is possible to connect to a PC only with a normal cable and to connect to another device only with a cross cable.

**No:** It is possible to connect to a PC only with a cross cable and to connect to another device only with a normal cable.

**Example**

In the following example, automatic crossover is enabled on port 1/e5.

```
Console(config)# interface ethernet 1/e5
Console(config-if)# mdix auto
```
**back-pressure**

The **back-pressure** Interface Configuration (Ethernet, port-channel) mode command enables back pressure on a given interface. To disable back pressure, use the **no** form of this command.

**Syntax**

- `back-pressure`
- `no back-pressure`

**Parameters**

There are no parameters for this command.

**Default Setting**

Back pressure is disabled.

**Command Mode**

Interface Configuration (Ethernet, port-channel) mode

**Command Usage**

There are no user guidelines for this command.

**Example**

In the following example, back pressure is enabled on port 1/e5.

```
Console(config)# interface ethernet 1/e5
Console(config-if)# back-pressure
```
clear counters

The **clear counters** User EXEC mode command clears statistics on an interface.

**Syntax**

clear counters [ethernet interface | port-channel port-channel-number]

**Parameters**

- *interface* — Valid Ethernet port. (Full syntax: port)
- *port-channel-number* — Valid port-channel number.

**Default Setting**

This command has no default configuration.

**Command Mode**

User EXEC mode

**Command Usage**

There are no user guidelines for this command.

**Example**

In the following example, the counters for interface 1/e1 are cleared.

```console
Console> clear counters ethernet 1/e1
```
set interface active

The set interface active Privileged EXEC mode command reactivates an interface that was shutdown.

Syntax

set interface active {ethernet interface | port-channel port-channel-number}

Parameters

- interface — Valid Ethernet port. (Full syntax: port)
- port-channel-number — Valid port-channel number.

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

This command is used to activate interfaces that were configured to be active, but were shut down by the system for some reason (for example, port security).

Example

The following command reactivates interface 1/e5.

```
Console# set interface active ethernet 1/e5
```
show interfaces advertise

The show interfaces advertise Privileged EXEC mode command displays auto negotiation data.

Syntax

show interfaces advertise [ethernet interface | port-channel port-channel-number]

Parameters

- interface — Valid Ethernet port. (Full syntax: port)
- port-channel-number — Valid port-channel number.

Default Setting

This command has no default configuration.

Command Modes

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following command displays auto negotiation information.

<table>
<thead>
<tr>
<th>Port</th>
<th>Type</th>
<th>Neg</th>
<th>Operational Link Advertisement</th>
</tr>
</thead>
<tbody>
<tr>
<td>---</td>
<td>----------</td>
<td>-------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>e1</td>
<td>100M-Copper</td>
<td>Enabled</td>
<td>--</td>
</tr>
<tr>
<td>e2</td>
<td>100M-Copper</td>
<td>Enabled</td>
<td>--</td>
</tr>
<tr>
<td>e3</td>
<td>100M-Copper</td>
<td>Enabled</td>
<td>--</td>
</tr>
<tr>
<td>e4</td>
<td>100M-Copper</td>
<td>Enabled</td>
<td>--</td>
</tr>
<tr>
<td>e5</td>
<td>100M-Copper</td>
<td>Enabled</td>
<td>100f, 100h, 10f, 10h</td>
</tr>
<tr>
<td>e6</td>
<td>100M-Copper</td>
<td>Enabled</td>
<td>--</td>
</tr>
<tr>
<td>e7</td>
<td>100M-Copper</td>
<td>Enabled</td>
<td>--</td>
</tr>
<tr>
<td>e8</td>
<td>100M-Copper</td>
<td>Enabled</td>
<td>--</td>
</tr>
<tr>
<td>e9</td>
<td>100M-Copper</td>
<td>Enabled</td>
<td>--</td>
</tr>
<tr>
<td>e10</td>
<td>100M-Copper</td>
<td>Enabled</td>
<td>--</td>
</tr>
<tr>
<td>e11</td>
<td>100M-Copper</td>
<td>Enabled</td>
<td>--</td>
</tr>
<tr>
<td>e12</td>
<td>100M-Copper</td>
<td>Enabled</td>
<td>--</td>
</tr>
<tr>
<td>e13</td>
<td>100M-Copper</td>
<td>Enabled</td>
<td>--</td>
</tr>
<tr>
<td>e14</td>
<td>100M-Copper</td>
<td>Enabled</td>
<td>--</td>
</tr>
<tr>
<td>e15</td>
<td>100M-Copper</td>
<td>Enabled</td>
<td>--</td>
</tr>
<tr>
<td>e16</td>
<td>100M-Copper</td>
<td>Enabled</td>
<td>--</td>
</tr>
</tbody>
</table>
show interfaces configuration

The show interfaces configuration Privileged EXEC mode command displays the configuration for all configured interfaces.

Syntax

show interfaces configuration [ethernet interface | port-channel port-channel-number]

Parameters

■ interface — Valid Ethernet port. (Full syntax: port)
■ port-channel-number — Valid port-channel number.

Default Setting

This command has no default configuration.

Command Modes

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following command displays the configuration of all configured interfaces:

```
Console# show interfaces configuration

<table>
<thead>
<tr>
<th>Port</th>
<th>Type</th>
<th>Duplex</th>
<th>Speed</th>
<th>Neg</th>
<th>Flow Ctrl</th>
<th>Link State</th>
<th>Back Pressure</th>
<th>Mdix Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>----</td>
<td>--------------</td>
<td>--------</td>
<td>-------</td>
<td>-----</td>
<td>-----------</td>
<td>-------------</td>
<td>---------------</td>
<td>-----------</td>
</tr>
<tr>
<td>1/e1</td>
<td>100M-Copper</td>
<td>Full</td>
<td>100</td>
<td>Enabled</td>
<td>Off</td>
<td>Up</td>
<td>Disabled</td>
<td>Auto</td>
</tr>
<tr>
<td>1/e2</td>
<td>100M-Copper</td>
<td>Full</td>
<td>100</td>
<td>Enabled</td>
<td>Off</td>
<td>Up</td>
<td>Disabled</td>
<td>Auto</td>
</tr>
<tr>
<td>1/e3</td>
<td>100M-Copper</td>
<td>Full</td>
<td>100</td>
<td>Enabled</td>
<td>Off</td>
<td>Up</td>
<td>Disabled</td>
<td>Auto</td>
</tr>
<tr>
<td>1/e4</td>
<td>100M-Copper</td>
<td>Full</td>
<td>100</td>
<td>Enabled</td>
<td>Off</td>
<td>Up</td>
<td>Disabled</td>
<td>Auto</td>
</tr>
<tr>
<td>1/e5</td>
<td>100M-Copper</td>
<td>Full</td>
<td>100</td>
<td>Enabled</td>
<td>Off</td>
<td>Up</td>
<td>Disabled</td>
<td>Auto</td>
</tr>
<tr>
<td>1/e6</td>
<td>100M-Copper</td>
<td>Full</td>
<td>100</td>
<td>Enabled</td>
<td>Off</td>
<td>Up</td>
<td>Disabled</td>
<td>Auto</td>
</tr>
<tr>
<td>1/e7</td>
<td>100M-Copper</td>
<td>Full</td>
<td>100</td>
<td>Enabled</td>
<td>Off</td>
<td>Up</td>
<td>Disabled</td>
<td>Auto</td>
</tr>
<tr>
<td>1/e8</td>
<td>100M-Copper</td>
<td>Full</td>
<td>100</td>
<td>Enabled</td>
<td>Off</td>
<td>Up</td>
<td>Disabled</td>
<td>Auto</td>
</tr>
<tr>
<td>1/e9</td>
<td>100M-Copper</td>
<td>Full</td>
<td>100</td>
<td>Enabled</td>
<td>Off</td>
<td>Up</td>
<td>Disabled</td>
<td>Auto</td>
</tr>
<tr>
<td>1/e10</td>
<td>100M-Copper</td>
<td>Full</td>
<td>100</td>
<td>Enabled</td>
<td>Off</td>
<td>Up</td>
<td>Disabled</td>
<td>Auto</td>
</tr>
<tr>
<td>1/e11</td>
<td>100M-Copper</td>
<td>Full</td>
<td>100</td>
<td>Enabled</td>
<td>Off</td>
<td>Up</td>
<td>Disabled</td>
<td>Auto</td>
</tr>
<tr>
<td>1/e12</td>
<td>100M-Copper</td>
<td>Full</td>
<td>100</td>
<td>Enabled</td>
<td>Off</td>
<td>Up</td>
<td>Disabled</td>
<td>Auto</td>
</tr>
<tr>
<td>1/e13</td>
<td>100M-Copper</td>
<td>Full</td>
<td>100</td>
<td>Enabled</td>
<td>Off</td>
<td>Up</td>
<td>Disabled</td>
<td>Auto</td>
</tr>
<tr>
<td>1/e14</td>
<td>100M-Copper</td>
<td>Full</td>
<td>100</td>
<td>Enabled</td>
<td>Off</td>
<td>Up</td>
<td>Disabled</td>
<td>Auto</td>
</tr>
<tr>
<td>1/e15</td>
<td>100M-Copper</td>
<td>Full</td>
<td>100</td>
<td>Enabled</td>
<td>Off</td>
<td>Up</td>
<td>Disabled</td>
<td>Auto</td>
</tr>
<tr>
<td>1/e16</td>
<td>100M-Copper</td>
<td>Full</td>
<td>100</td>
<td>Enabled</td>
<td>Off</td>
<td>Up</td>
<td>Disabled</td>
<td>Auto</td>
</tr>
</tbody>
</table>
```
show interfaces status

The show interfaces status Privileged EXEC mode command displays the status of all configured interfaces.

Syntax

show interfaces status [ethernet interface|port-channel port-channel-number]

Parameters

- interface — A valid Ethernet port. (Full syntax: port)
- port-channel-number — A valid port-channel number.

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following command displays the status of all configured interfaces:

```
Console# show interfaces status

<table>
<thead>
<tr>
<th>Port</th>
<th>Type</th>
<th>Duplex</th>
<th>Speed</th>
<th>Neg</th>
<th>Flow Ctrl</th>
<th>Link State</th>
<th>Back Pressure</th>
<th>Mdix Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>----</td>
<td>-------------</td>
<td>------</td>
<td>-------</td>
<td>-----</td>
<td>----------</td>
<td>------------</td>
<td>--------------</td>
<td>-----------</td>
</tr>
<tr>
<td>1/e1</td>
<td>100M-Copper</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>Down</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>1/e2</td>
<td>100M-Copper</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>Down</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>1/e3</td>
<td>100M-Copper</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>Down</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>1/e4</td>
<td>100M-Copper</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>Down</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>1/e5</td>
<td>100M-Copper</td>
<td>Full</td>
<td>100</td>
<td>Enabled</td>
<td>Off</td>
<td>Up</td>
<td>Disabled</td>
<td>Auto</td>
</tr>
<tr>
<td>1/e6</td>
<td>100M-Copper</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>Down</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>1/e7</td>
<td>100M-Copper</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>Down</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>1/e8</td>
<td>100M-Copper</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>Down</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>1/e9</td>
<td>100M-Copper</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>Down</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>1/e10</td>
<td>100M-Copper</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>Down</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>1/e11</td>
<td>100M-Copper</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>Down</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>1/e12</td>
<td>100M-Copper</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>Down</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>1/e13</td>
<td>100M-Copper</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>Down</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>1/e14</td>
<td>100M-Copper</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>Down</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>1/e15</td>
<td>100M-Copper</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>Down</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>1/e16</td>
<td>100M-Copper</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>Down</td>
<td>--</td>
<td>--</td>
</tr>
</tbody>
</table>
```
show interfaces description

The show interfaces description Privileged EXEC mode command displays the description for all configured interfaces.

Syntax

show interfaces description [ethernet interface | port-channel port-channel-number]

Parameters

- interface — Valid Ethernet port. (Full syntax: port)
- port-channel-number — A valid port-channel number.

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following command displays descriptions of configured interfaces:

```
Console# show interfaces description

Port Description
----  -----------
1/e1  lab
1/e2
1/e3
1/e4
1/e5
1/e6
ch1
ch2
```
show interfaces counters

The show interfaces counters User EXEC mode command displays traffic seen by the physical interface.

**Syntax**

`show interfaces counters [ethernet interface | port-channel port-channel-number]`

**Parameters**

- `interface` — A valid Ethernet port. (Full syntax: `port`)
- `port-channel-number` — A valid port-channel number.

**Default Setting**

This command has no default configuration.

**Command Mode**

User EXEC mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command displays traffic seen by the physical interface:

```
Console# show interfaces counters

<table>
<thead>
<tr>
<th></th>
<th>InOctets</th>
<th>InUcastPkts</th>
<th>InMcastPkts</th>
<th>InBcastPkts</th>
</tr>
</thead>
<tbody>
<tr>
<td>---</td>
<td>---------</td>
<td>------------</td>
<td>------------</td>
<td>------------</td>
</tr>
<tr>
<td>1/e1</td>
<td>183892</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2/e1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3/e1</td>
<td>123899</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>OutOctets</th>
<th>OutUcastPkts</th>
<th>OutMcastPkts</th>
<th>OutBcastPkts</th>
</tr>
</thead>
<tbody>
<tr>
<td>---</td>
<td>-----------</td>
<td>--------------</td>
<td>--------------</td>
<td>--------------</td>
</tr>
<tr>
<td>1/e1</td>
<td>9188</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2/e1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3/e1</td>
<td>8789</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>InOctets</th>
<th>InUcastPkts</th>
<th>InMcastPkts</th>
<th>InBcastPkts</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>27889</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>OutOctets</th>
<th>OutUcastPkts</th>
<th>OutMcastPkts</th>
<th>OutBcastPkts</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>23739</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```
The following command displays counters for Ethernet port 1/e1:

```
Console# show interfaces counters ethernet 1/e1
```

<table>
<thead>
<tr>
<th>Port</th>
<th>InOctets</th>
<th>InUcastPkts</th>
<th>InMcastPkts</th>
<th>InBcastPkts</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/e1</td>
<td>183892</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>OutOctets</th>
<th>OutUcastPkts</th>
<th>OutMcastPkts</th>
<th>OutBcastPkts</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/e1</td>
<td>9188</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

FCS Errors: 8
Single Collision Frames: 0
Late Collisions: 0
Oversize Packets: 0
Internal MAC Rx Errors: 0
Symbol Errors: 0
Received Pause Frames: 0
Transmitted Pause Frames: 0

The following table describes the fields shown in the example.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InOctets</td>
<td>Counted received octets.</td>
</tr>
<tr>
<td>InUcastPkts</td>
<td>Counted received unicast packets.</td>
</tr>
<tr>
<td>InMcastPkts</td>
<td>Counted received multicast packets.</td>
</tr>
<tr>
<td>InBcastPkts</td>
<td>Counted received broadcast packets.</td>
</tr>
<tr>
<td>OutOctets</td>
<td>Counted transmitted octets.</td>
</tr>
<tr>
<td>OutUcastPkts</td>
<td>Counted transmitted unicast packets.</td>
</tr>
<tr>
<td>OutMcastPkts</td>
<td>Counted transmitted multicast packets.</td>
</tr>
<tr>
<td>OutBcastPkts</td>
<td>Counted transmitted broadcast packets.</td>
</tr>
<tr>
<td>FCS Errors</td>
<td>Counted received frames that are an integral number of octets in length but do not pass the FCS check.</td>
</tr>
<tr>
<td>Single Collision Frames</td>
<td>Counted frames that are involved in a single collision, and are subsequently transmitted successfully.</td>
</tr>
<tr>
<td>Late Collisions</td>
<td>Number of times that a collision is detected later than one slot time into the transmission of a packet.</td>
</tr>
<tr>
<td>Oversize Packets</td>
<td>Counted frames received that exceed the maximum permitted frame size.</td>
</tr>
<tr>
<td>Internal MAC Rx Errors</td>
<td>Counted frames for which reception fails due to an internal MAC sublayer receive error.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Received Pause Frames</td>
<td>Counted MAC Control frames received with an opcode indicating the PAUSE operation.</td>
</tr>
<tr>
<td>Transmitted Pause Frames</td>
<td>Counted MAC Control frames transmitted on this interface with an opcode indicating the PAUSE operation.</td>
</tr>
</tbody>
</table>
**port storm-control include-multicast (IC)**

The `port storm-control include-multicast` Interface Configuration (Ethernet) mode command counts multicast packets in broadcast storm control. To disable counting multicast packets, use the `no` form of this command.

**Syntax**

```
port storm-control include-multicast [unknown-unicast]
no port storm-control include-multicast
```

**Parameters**

- `unknown-unicast` — Specifies also counting unknown unicast packets.

**Default Setting**

Multicast packets are not counted.

**Command Mode**

Interface Configuration (Ethernet) mode

**Command Usage**

To control multicasts storms, use the `port storm-control broadcast enable` and `port storm-control broadcast rate` commands.

**Example**

The following command enables counting broadcast and multicast packets on Ethernet port 2/e3.

```
Console(config)# interface ethernet 2/e3
Console(config-if)# port storm-control include-multicast
```
**port storm-control broadcast enable**

The **port storm-control broadcast enable** Interface Configuration (Ethernet) mode command enables broadcast storm control. To disable broadcast storm control, use the **no** form of this command.

**Syntax**

```
port storm-control broadcast enable
no port storm-control broadcast enable
```

**Parameters**

There are no parameters for this command.

**Default Setting**

Broadcast storm control is disabled.

**Command Mode**

Interface Configuration (Ethernet) mode

**Command Usage**

Use the **port storm-control broadcast rate** Interface Configuration (Ethernet) mode command, to set the maximum allowable broadcast rate.

**Example**

The following command enables broadcast storm control on port 1/g5 of a device.

```
Console(config)# interface ethernet 1/g5
Console(config)# port storm-control broadcast enable
```
port storm-control broadcast rate

The **port storm-control broadcast rate** Interface Configuration (Ethernet) mode command configures the maximum broadcast rate. To return to the default configuration, use the **no** form of this command.

**Syntax**

```
port storm-control broadcast rate rate
no port storm-control broadcast rate
```

**Parameters**

- **rate** — Maximum kilobits per second of broadcast and multicast traffic on a port. (Range: 70-100000).

**Default Setting**

The default storm control broadcast rate is 3500 Kbits/Sec.

**Command Mode**

Interface Configuration (Ethernet) mode

**Command Usage**

Use the **port storm-control broadcast enable** Interface Configuration mode command to enable broadcast storm control.

**Example**

The following command configures the maximum storm control broadcast rate at 900 Kbits/Sec on Ethernet port 1/e5 of a device.

```
Console(config)# interface ethernet 1/e5
Console(config-if)# port storm-control broadcast rate 900
```
show ports storm-control

The `show ports storm-control` User EXEC mode command displays the storm control configuration.

**Syntax**

`show ports storm-control [interface]`

**Parameters**

- `interface` — A valid Ethernet port. (Full syntax: `port`)

**Default Setting**

This command has no default configuration.

**Command Mode**

User EXEC mode.

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command displays the storm control configuration.

```
Console# show ports storm-control
Port   State  Rate [Kbits/Sec] Included
-----   ------   --------------  ------------------------------
 1/e1   Enabled  70            Broadcast, Multicast, Unknown Unicast
 2/e1   Enabled  100           Broadcast
 3/e1   Disabled 100           Broadcast
```
gvrp enable (Global)

GARP VLAN Registration Protocol (GVRP) is an industry-standard protocol designed to propagate VLAN information from device to device. With GVRP, a single device is manually configured with all desired VLANs for the network, and all other devices on the network learn these VLANs dynamically.

The gvrp enable Global Configuration mode command enables GVRP globally. To disable GVRP on the device, use the no form of this command.

Syntax

```
gvrp enable
no gvrp enable
```

Parameters

There are no parameters for this command.

Default Setting

GVRP is globally disabled.

Command Mode

Global Configuration mode

Command Usage

There are no user guidelines for this command.

Example

The following command enables GVRP globally on the device.

```
Console(config)# gvrp enable
```
gvrp enable (Interface)

The `gvrp enable` Interface Configuration (Ethernet, port-channel) mode command enables GVRP on an interface. To disable GVRP on an interface, use the `no` form of this command.

**Syntax**

```
gvrp enable
no gvrp enable
```

**Parameters**

There are no parameters for this command.

**Default Setting**

GVRP is disabled on all interfaces.

**Command Mode**

Interface Configuration (Ethernet, port-channel) mode

**Command Usage**

An access port does not dynamically join a VLAN because it is always a member in only one VLAN.

Membership in an untagged VLAN is propagated in the same way as in a tagged VLAN. That is, the PVID is manually defined as the untagged VLAN VID.

**Example**

The following command enables GVRP on Ethernet port 1/e6.

```
Console(config)# interface ethernet 1/e6
Console(config-if)# gvrp enable
```
garp timer

The `garp timer` Interface Configuration (Ethernet, port-channel) mode command adjusts the values of the join, leave, and leaveall timers of GARP applications. To return to the default configuration, use the `no` form of this command.

**Syntax**

```
garp timer {join | leave | leaveall} timer_value
no garp timer
```

**Parameters**

- `{join | leave | leaveall}` — Indicates the type of timer.
- `timer_value` — Timer values in milliseconds in multiples of 10. (Range: 10-2147483647)

**Default Setting**

Following are the default timer values:

- Join timer — 200 milliseconds
- Leave timer — 600 milliseconds
- Leaveall timer — 10000 milliseconds

**Command Mode**

Interface configuration (Ethernet, port-channel) mode

**Command Usage**

The following relationship must be maintained between the timers:

- Leave time must be greater than or equal to three times the join time.
- Leave-all time must be greater than the leave time.
- Set the same GARP timer values on all Layer 2-connected devices. If the GARP timers are set differently on Layer 2-connected devices, the GARP application will not operate successfully.

**Example**

In the following example, the leave timer for Ethernet port 1/e6 is set to 900 milliseconds.

```
Console(config)# interface ethernet 1/e6
Console(config-if)# garp timer leave 900
```
**gvrp vlan-creation-forbid**

The `gvrp vlan-creation-forbid` Interface Configuration (Ethernet, port-channel) mode command disables dynamic VLAN creation or modification. To enable dynamic VLAN creation or modification, use the `no` form of this command.

**Syntax**

```plaintext
gvrp vlan-creation-forbid
no gvrp vlan-creation-forbid
```

**Parameters**

There are no parameters for this command.

**Default Setting**

Dynamic VLAN creation or modification is enabled.

**Command Mode**

Interface Configuration (Ethernet, port-channel) mode

**Command Usage**

This command forbids dynamic VLAN creation from the interface. The creation or modification of dynamic VLAN registration entries as a result of the GVRP exchanges on an interface are restricted only to those VLANs for which static VLAN registration exists.

**Example**

The following command disables dynamic VLAN creation on Ethernet port 1/e6.

```plaintext
Console(config)# interface ethernet 1/e6
Console(config-if)# gvrp vlan-creation-forbid
```
gvrp registration-forbid

The `gvrp registration-forbid` Interface Configuration (Ethernet, port-channel) mode command de-registers all dynamic VLANs on a port and prevents VLAN creation or registration on the port. To allow dynamic registration of VLANs on a port, use the `no` form of this command.

**Syntax**

```plaintext
gvrp registration-forbid
no gvrp registration-forbid
```

**Parameters**

There are no parameters for this command.

**Default Setting**

Dynamic registration of VLANs on the port is allowed.

**Command Mode**

Interface Configuration (Ethernet, port-channel) mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command forbids dynamic registration of VLANs on Ethernet port 1/e6.

```plaintext
Console(config)# interface ethernet 1/e6
Console(config-if)# gvrp registration-forbid
```
clear gvrp statistics

The **clear gvrp statistics** Privileged EXEC mode command clears all GVRP statistical information.

**Syntax**

clear gvrp statistics [ethernet interface | port-channel port-channel-number]

**Parameters**

- **interface** — A valid Ethernet port. (Full syntax: port)
- **port-channel-number** — A valid port-channel number.

**Default Setting**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command clears all GVRP statistical information on Ethernet port 1/e6.

```console
Console# clear gvrp statistics ethernet 1/e6
```
**show gvrp configuration**

The **show gvrp configuration** User EXEC mode command displays GVRP configuration information, including timer values, whether GVRP and dynamic VLAN creation is enabled, and which ports are running GVRP.

**Syntax**

```
show gvrp configuration [ethernet interface | port-channel port-channel-number]
```

**Parameters**

- `interface` — A valid Ethernet port. (Full syntax: `port`)
- `port-channel-number` — A valid port-channel number.

**Default Setting**

This command has no default configuration.

**Command Mode**

User EXEC mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command displays GVRP configuration information:

```
Console> show gvrp configuration

GVRP Feature is currently enabled on the device.

<table>
<thead>
<tr>
<th>Port(s)</th>
<th>Status</th>
<th>Registration</th>
<th>Dynamic VLAN Creation</th>
<th>Timers (milliseconds)</th>
<th>Leave All</th>
</tr>
</thead>
<tbody>
<tr>
<td>-------</td>
<td>--------</td>
<td>--------------</td>
<td>-----------------------</td>
<td>-----------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>2/e1</td>
<td>Enabled</td>
<td>Normal</td>
<td>Enabled</td>
<td>200 600 10000</td>
<td></td>
</tr>
<tr>
<td>4/e4</td>
<td>Enabled</td>
<td>Normal</td>
<td>Enabled</td>
<td>200 600 10000</td>
<td></td>
</tr>
</tbody>
</table>
```
show gvrp statistics

The **show gvrp statistics** User EXEC mode command displays GVRP statistics.

**Syntax**

```
show gvrp statistics [ethernet interface | port-channel port-channel-number]
```

**Parameters**

- **interface** — A valid Ethernet port. (Full syntax: *port*)
- **port-channel-number** — A valid port-channel number.

**Default Setting**

This command has no default configuration.

**Command Mode**

User EXEC mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command shows GVRP statistical information:

```
Console> show gvrp statistics

GVRP Statistics:
Legend:
 rJE : Join Empty Received  rJIn: Join In Received
 rEmp : Empty Received       rLin: Leave In Received
 rLE : Leave Empty Received  rLA : Leave All Received
 sJE : Join Empty Sent       sJIn: Join In Sent
 sEmp : Empty Sent           sLin: Leave In Sent
 sLE : Leave Empty Sent      sLA : Leave All Sent
Port  rJE rJIn rEmp rLin  rLE  rLA  sJE sJIn sEmp sLin sLE  sLA
```
**show gvrp error-statistics**

The `show gvrp error-statistics` User EXEC mode command displays GVRP error statistics.

**Syntax**

```
show gvrp error-statistics [ethernet interface | port-channel port-channel-number]
```

**Parameters**

- `interface` — A valid Ethernet port. (Full syntax: `port`)
- `port-channel-number` — A valid port-channel number.

**Default Setting**

This command has no default configuration.

**Command Mode**

User EXEC mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command displays GVRP statistical information.

```
Console> show gvrp error-statistics

GVRP Error Statistics:
Legend:

<table>
<thead>
<tr>
<th>INVPROT:</th>
<th>Invalid Protocol Id</th>
<th>INVALEN:</th>
<th>Invalid Attribute Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>INVATYP:</td>
<td>Invalid Attribute Type</td>
<td>INVEVENT:</td>
<td>Invalid Event</td>
</tr>
<tr>
<td>INVAVAL:</td>
<td>Invalid Attribute Value</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Port INVPROT INVATYP INVAVAL INVALEN INVEVENT
```
**ip igmp snooping (Global)**

The **ip igmp snooping** Global Configuration mode command enables Internet Group Management Protocol (IGMP) snooping. To disable IGMP snooping, use the **no** form of this command.

**Syntax**

```plaintext
ip igmp snooping
no ip igmp snooping
```

**Parameters**

There are no parameters for this command.

**Default Setting**

IGMP snooping is disabled.

**Command Mode**

Global Configuration mode

**Command Usage**

IGMP snooping can only be enabled on static VLANs. It must not be enabled on Private VLANs or their community VLANs.

**Example**

The following command enables IGMP snooping.

```
Console(config)# ip igmp snooping
```
**ip igmp snooping (Interface)**

The **ip igmp snooping** Interface Configuration (VLAN) mode command enables Internet Group Management Protocol (IGMP) snooping on a specific VLAN. To disable IGMP snooping on a VLAN interface, use the **no** form of this command.

**Syntax**

```
ip igmp snooping
no ip igmp snooping
```

**Parameters**

There are no parameters for this command.

**Default Setting**

IGMP snooping is disabled.

**Command Mode**

Interface Configuration (VLAN) mode

**Command Usage**

IGMP snooping can only be enabled on static VLANs. It must not be enabled on Private VLANs or their community VLANs.

**Example**

The following command enables IGMP snooping on VLAN 2.

```
Console(config)# interface vlan 2
Console(config-if)# ip igmp snooping
```
nip igmp snooping host-time-out

The **ip igmp snooping host-time-out** Interface Configuration (VLAN) mode command configures the host-time-out. If an IGMP report for a multicast group was not received for a host-time-out period from a specific port, this port is deleted from the member list of that multicast group. To return to the default configuration, use the **no** form of this command.

**Syntax**

```
ip igmp snooping host-time-out  time-out
no ip igmp snooping host-time-out
```

**Parameters**

- **time-out** — Host timeout in seconds. (Range: 1-2147483647)

**Default Setting**
The default host-time-out is 260 seconds.

**Command Mode**

Interface Configuration (VLAN) mode

**Command Usage**
The timeout should be at least greater than 2*query_interval+max_response_time of the IGMP router.

**Example**

In the following example, the host timeout is configured to 300 seconds.

```
Console(config)# interface vlan 2
Console(config-if)# ip igmp snooping host-time-out 300
```
ip igmp snooping mrouter-time-out

The `ip igmp snooping mrouter-time-out` Interface Configuration (VLAN) mode command configures the mrouter-time-out. The `ip igmp snooping mrouter-time-out` Interface Configuration (VLAN) mode command is used for setting the aging-out time after multicast device ports are automatically learned. To return to the default configuration, use the `no` form of this command.

**Syntax**

```plaintext
ip igmp snooping mrouter-time-out time-out
no ip igmp snooping mrouter-time-out
```

**Parameters**

- `time-out` — Multicast device timeout in seconds. (Range: 1-2147483647)

**Default Setting**

The default value is 300 seconds.

**Command Mode**

Interface Configuration (VLAN) mode

**Command Usage**

There are no user guidelines for this command.

**Example**

In the following example, the multicast device timeout is configured to 200 seconds.

```plaintext
Console(config)# interface vlan 2
Console(config-if)# ip igmp snooping mrouter-time-out 200
```
**ip igmp snooping mrouter learn-pim-dvmrp**

The `ip igmp snooping mrouter learn-pim-dvmrp` Interface Configuration (VLAN) mode command enables automatic learning of multicast router ports in the context of a specific VLAN. To remove automatic learning of multi-cast router ports, use the `no` form of this command.

**Syntax**

- `ip igmp snooping mrouter learn-pim-dvmrp`
- `no ip igmp snooping mrouter learn-pim-dvmrp`

**Default Configuration**

Automatic learning of multicast router ports is enabled.

**Command Mode**

Interface Configuration (VLAN) mode

**User Guidelines**

There are no user guidelines for this command.

**Example**

The following command enables automatic learning of multicast router ports on VLAN 2.

```
Console(config)# interface vlan 2
Console(config-if)# ip igmp snooping mrouter learn-pim-dvmrp
```
**ip igmp snooping leave-time-out**

The **ip igmp snooping leave-time-out** Interface Configuration (VLAN) mode command configures the leave-time-out. If an IGMP report for a multicast group was not received for a leave-time-out period after an IGMP Leave was received from a specific port, this port is deleted from the member list of that multicast group. To return to the default configuration, use the **no** form of this command.

**Syntax**

```
ip igmp snooping leave-time-out {time-out | immediate-leave}
no ip igmp snooping leave-time-out
```

**Parameters**

- **time-out** — Specifies the leave-time-out in seconds for IGMP queries.
  (Range: 0-2147483647)
- **immediate-leave** — Indicates that the port should be immediately removed from the members list after receiving IGMP Leave.

**Default Setting**

The default leave-time-out configuration is 10 seconds.

**Command Mode**

Interface Configuration (VLAN) mode

**Command Usage**

The leave time-out should be set greater than the maximum time that a host is allowed to respond to an IGMP query.

Use **immediate leave** only where there is just one host connected to a port.

**Example**

The following command configures the host leave-time-out to 60 seconds.

```
Console(config)# interface vlan 2
Console(config-if)# ip igmp snooping leave-time-out 60
```
show ip igmp snooping mrouter

The `show ip igmp snooping mrouter` User EXEC mode command displays information on dynamically learned multicast device interfaces.

**Syntax**

```
show ip igmp snooping mrouter [interface vlan-id]
```

**Parameters**

- `vlan-id` — VLAN number.

**Default Setting**

This command has no default configuration.

**Command Mode**

User EXEC mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command displays multicast device interfaces in VLAN 1000.

```
Console> show ip igmp snooping mrouter interface 1000

VLAN   Ports
------ -----
     1000 1/e1

Detected multicast routers that are forbidden statically:

VLAN   Ports
------ -----
     1000 1/e19
```
show ip igmp snooping interface

The `show ip igmp snooping interface` User EXEC mode command displays IGMP snooping configuration.

**Syntax**

`show ip igmp snooping interface vlan-id`

**Parameters**

- `vlan-id` — VLAN number.

**Default Setting**

This command has no default configuration.

**Command Mode**

User EXEC mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command displays IGMP snooping information on VLAN 1000.

```
Console> show ip igmp snooping interface 1000

IGMP Snooping is globally enabled
IGMP Snooping is enabled on VLAN 1000
IGMP host timeout is 300 sec
IGMP Immediate leave is disabled. IGMP leave timeout is 10 sec
IGMP mrouter timeout is 200 sec
Automatic learning of multicast router ports is enabled
```
show ip igmp snooping groups

The `show ip igmp snooping groups` User EXEC mode command displays multicast groups learned by IGMP snooping.

**Syntax**

```
show ip igmp snooping groups [vlan vlan-id] [address ip-multicast-address]
```

**Parameters**

- `vlan-id` — VLAN number.
- `ip-multicast-address` — IP multicast address.

**Default Setting**

This command has no default configuration.

**Command Mode**

User EXEC mode

**Command Usage**

To see the full multicast address table (including static addresses) use the `show bridge multicast address-table` Privileged EXEC command.

**Example**

The following command shows IGMP snooping information on multicast groups.

```
Console> show ip igmp snooping groups

<table>
<thead>
<tr>
<th>VLAN</th>
<th>IP Address</th>
<th>Querier</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>----</td>
<td>-------------------</td>
<td>-------</td>
<td>---------</td>
</tr>
<tr>
<td>1</td>
<td>224-239.130/2.2.3</td>
<td>Yes</td>
<td>1/e1, 2/e2</td>
</tr>
<tr>
<td>19</td>
<td>224-239.130/2.2.8</td>
<td>Yes</td>
<td>1/e9-e11</td>
</tr>
</tbody>
</table>

IGMP Reporters that are forbidden statically:

<table>
<thead>
<tr>
<th>VLAN</th>
<th>IP Address</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>----</td>
<td>-------------------</td>
<td>-----</td>
</tr>
<tr>
<td>1</td>
<td>224-239.130/2.2.3</td>
<td>1/e19</td>
</tr>
</tbody>
</table>
```
### ip address

The `ip address` Interface Configuration (Ethernet, VLAN, port-channel) mode command sets an IP address. To remove an IP address, use the `no` form of this command.

**Syntax**

```
ip address ip-address {mask | prefix-length}
no ip address [ip-address]
```

**Parameters**

- `ip-address` — Valid IP address
- `mask` — Valid network mask of the IP address.
- `prefix-length` — Specifies the number of bits that comprise the IP address prefix. The prefix length must be preceded by a forward slash (/). (Range: 8-30)

**Default Setting**

Two interfaces are configured:

- one for VLAN 1
- one for VLAN 2, with DHCP set by default

**Command Mode**

Interface Configuration (Ethernet, VLAN, port-channel) mode

**Command Usage**

An IP address cannot be configured for a range of interfaces (range context).

**Example**

The following command configures VLAN 1 with IP address 131.108.1.27 and subnet mask 255.255.255.0.

```
Console(config)# interface vlan 1
Console(config-if)# ip address 131.108.1.27 255.255.255.0
```
ip address dhcp

The ip address dhcp Interface Configuration (Ethernet, VLAN, port-channel) mode command acquires an IP address for an Ethernet interface from the Dynamic Host Configuration Protocol (DHCP) server. To deconfigure an acquired IP address, use the no form of this command.

Syntax

ip address dhcp [hostname host-name]
no ip address dhcp

Parameters

- **host-name** — Specifies the name of the host to be placed in the DHCP option 12 field. This name does not have to be the same as the host name specified in the hostname Global Configuration mode command. (Range: 1-20 characters)

Default Setting

This command has no default configuration.

Command Mode

Interface Configuration (Ethernet, VLAN, port-channel) mode

Command Usage

The **ip address dhcp** command allows any interface to dynamically learn its IP address by using the DHCP protocol.

Some DHCP servers require that the DHCPDISCOVER message have a specific host name. The **ip address dhcp hostname host-name** command is most typically used when the host name is provided by the system administrator.

If the device is configured to obtain its IP address from a DHCP server, it sends a DHCPDISCOVER message to provide information about itself to the DHCP server on the network.

If the **ip address dhcp** command is used with or without the optional keyword, the DHCP option 12 field (host name option) is included in the DHCPDISCOVER message. By default, the specified DHCP host name is the globally configured host name of the device. However, the **ip address dhcp hostname host-name** command can be used to place a different host name in the DHCP option 12 field.

The **no ip address dhcp** command de-configures any IP address that was acquired, thus sending a DHCPRELEASE message.

Example

The following command acquires an IP address for Ethernet port 1/e16 from DHCP.

```
Console(config)# interface ethernet 1/e16
Console(config-if)# ip address dhcp
```
ip default-gateway

The ip default-gateway Global Configuration mode command defines a default gateway. To return to the default configuration, use the no form of this command.

Syntax

ip default-gateway ip-address
no ip default-gateway

Parameters

- ip-address — Valid IP address of the default gateway.

Default Setting

No default gateway is defined.

Command Mode

Global Configuration mode

Command Usage

There are no user guidelines for this command.

Example

The following command defines default gateway 192.168.1.1.

```
Console(config)# ip default-gateway 192.168.1.1
```
show ip interface

The `show ip interface` Privileged EXEC mode command displays the usability status of configured IP interfaces.

**Syntax**

`show ip interface [ethernet interface-number | vlan vlan-id | port-channel port-channel number]`

**Parameters**

- `interface-number` — Valid Ethernet port.
- `vlan-id` — Valid VLAN number.
- `port-channel number` — Valid port-channel number.

**Default Setting**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command displays the configured IP interfaces and their types.

```
Console# show ip interface

Gateway IP Address       Type  Activity Status
------------------ ------ ---------------
10.7.1.1               Static Active

IP address   Interface Type
----------   ------ ------
10.7.1.192/24 VLAN 1 Static
10.7.2.192/24 VLAN 2 DHCP
```
arp

The **arp** Global Configuration mode command adds a permanent entry in the Address Resolution Protocol (ARP) cache. To remove an entry from the ARP cache, use the **no** form of this command.

**Syntax**

```
arp ip_addr hw_addr {ethernet interface-number | vlan vlan-id | port-channel port-channel number}
```

```
no arp ip_addr {ethernet interface-number | vlan vlan-id | port-channel port-channel number}
```

**Parameters**

- **ip_addr** — Valid IP address or IP alias to map to the specified MAC address.
- **hw_addr** — Valid MAC address to map to the specified IP address or IP alias.
- **interface-number** — Valid Ethernet port.
- **vlan-id** — Valid VLAN number.
- **port-channel number** — Valid port-channel number.

**Default Setting**

This command has no default configuration.

**Command Mode**

Global Configuration mode

**Command Usage**

The software uses ARP cache entries to translate 32-bit IP addresses into 48-bit hardware addresses. Because most hosts support dynamic resolution, static ARP cache entries do not generally have to be specified.

**Example**

The following command adds IP address 198.133.219.232 and MAC address 00:00:0c:40:0f:bc to the ARP table.

```
Console(config)# arp 198.133.219.232 00:00:0c:40:0f:bc ethernet 1/e6
```
arp timeout

The arp timeout Global Configuration mode command configures how long an entry remains in the ARP cache. To return to the default configuration, use the no form of this command.

Syntax

arp timeout seconds
no arp timeout

Parameters

- seconds — Time (in seconds) that an entry remains in the ARP cache. (Range: 1-40000000)

Default Setting

The default timeout is 60000 seconds.

Command Mode

Global Configuration mode

Command Usage

It is recommended not to set the timeout value to less than 3600.

Example

The following command configures the ARP timeout to 12000 seconds.

```
Console(config)# arp timeout 12000
```
clear arp-cache

The clear arp-cache Privileged EXEC mode command deletes all dynamic entries from the ARP cache.

Syntax

clear arp-cache

Parameters

There are no parameters for this command.

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following command deletes all dynamic entries from the ARP cache.

```
Console# clear arp-cache
```
show arp

The show arp Privileged EXEC mode command displays entries in the ARP table.

Syntax

show arp

Parameters

There are no parameters for this command.

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following command displays entries in the ARP table.

```
Console# show arp

ARP timeout: 80000 Seconds

<table>
<thead>
<tr>
<th>Interface</th>
<th>IP address</th>
<th>HW address</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/e1</td>
<td>10.7.1.102</td>
<td>00:10:B5:04:DB:4B</td>
<td>Dynamic</td>
</tr>
<tr>
<td>2/e2</td>
<td>10.7.1.135</td>
<td>00:50:22:00:2A:44</td>
<td>Static</td>
</tr>
</tbody>
</table>
```
**ip domain-lookup**

The `ip domain-lookup` Global Configuration mode command enables the IP Domain Naming System (DNS)-based host name-to-address translation. To disable DNS-based host name-to-address translation, use the `no` form of this command.

**Syntax**

`ip domain-lookup`

`no ip domain-lookup`

**Parameters**

There are no parameters for this command.

**Default Setting**

IP Domain Naming System (DNS)-based host name-to-address translation is enabled.

**Command Mode**

Global Configuration mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command enables IP Domain Naming System (DNS)-based host name-to-address translation.

```
Console(config)# ip domain-lookup
```
ip domain-name

The **ip domain-name** Global Configuration mode command defines a default domain name used by the software to complete unqualified host names (names without a dotted-decimal domain name). To remove the default domain name, use the **no** form of this command.

**Syntax**

```
ip domain-name name
no ip domain-name
```

**Parameters**

- **name** — Specifies the default domain name used to complete unqualified host names. Do not include the initial period that separates an unqualified name from the domain name.
  
  (Range: 1-158 characters)

**Default Setting**

A default domain name is not defined.

**Command Mode**

Global Configuration mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command defines default domain name `www.Marvell.com`.

```console
Console(config)# ip domain-name www.Marvell.com
```
**ip name-server**

The `ip name-server` Global Configuration mode command defines the available name servers. To remove a name server, use the `no` form of this command.

**Syntax**

```
ip name-server server-address [server-address2 ... server-address8]
no ip name-server [server-address1 ... server-address8]
```

**Parameters**

- `server-address` — Specifies IP addresses of the name server.

**Default Setting**

No name server addresses are specified.

**Command Mode**

Global Configuration mode

**Command Usage**

The preference of the servers is determined by the order in which they were entered. Up to 8 servers can be defined using one command or using multiple commands.

**Example**

The following command sets the available name server.

```
Console(config)# ip name-server 176.16.1.18
```
ip host

The `ip host` Global Configuration mode command defines static host name-to-address mapping in the host cache. To remove the name-to-address mapping, use the `no` form of this command.

**Syntax**

```
ip host name address
no ip host name
```

**Parameters**

- `name` — Name of the host (Range: 1-158 characters)
- `address` — Associated IP address.

**Default Setting**

No host is defined.

**Command Mode**

Global Configuration mode

**Command Usage**

Up to 8 host names can be configured.

**Example**

The following command defines a static host name-to-address mapping in the host cache.

```
Console(config)# ip host accounting.Marvell.com 176.10.23.1
```
clear host

The **clear host** Privileged EXEC mode command deletes entries from the host name-to-address cache.

**Syntax**

```
clear host {name | *}
```

**Parameters**

- **name** — Specifies the host entry to be removed. (Range: 1-158 characters)
- ***** — Removes all entries.

**Default Setting**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command deletes all entries from the host name-to-address cache.

```
Console# clear host *
```
clear host dhcp

The clear host dhcp Privileged EXEC mode command deletes entries from the host name-to-address mapping received from Dynamic Host Configuration Protocol (DHCP).

Syntax

clear host dhcp {name | *}

Parameters

■ name — Specifies the host entry to be removed. (Range: 1-158 characters)
■ * — Removes all entries.

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

This command deletes the host name-to-address mapping temporarily until the next renewal of the IP address.

Example

The following command deletes all entries from the host name-to-address mapping.

```
Console# clear host dhcp *
```
**show hosts**

The **show hosts** Privileged EXEC mode command displays the default domain name, a list of name server hosts, the static and the cached list of host names and addresses.

**Syntax**

`show hosts [name]`

**Parameters**

- **name** — Specifies the host name. (Range: 1-158 characters)

**Default Setting**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command displays host information.

```
Console# show hosts

System name: Device
Default domain is gm.com, sales.gm.com, usa.sales.gm.com(DHCP)
Name/address lookup is enabled
Name servers (Preference order): 176.16.1.18 176.16.1.19

Configured host name-to-address mapping:

<table>
<thead>
<tr>
<th>Host</th>
<th>Addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>accounting.gm.com</td>
<td>176.16.8.8 176.16.8.9 (DHCP)</td>
</tr>
</tbody>
</table>

Cache:

<table>
<thead>
<tr>
<th>Host</th>
<th>TTL (Hours)</th>
<th>Total</th>
<th>Elapsed</th>
<th>Type</th>
<th>Addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>---</td>
<td>----</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="http://www.stanford.edu">www.stanford.edu</a></td>
<td>72</td>
<td>3</td>
<td></td>
<td>IP</td>
<td>171.64.14.203</td>
</tr>
</tbody>
</table>
The `lacp system-priority` Global Configuration mode command configures the system priority. To return to the default configuration, use the `no` form of this command.

**Syntax**

```
lacp system-priority value
no lacp system-priority
```

**Parameters**

- `value` — Specifies system priority value. (Range: 1-65535)

**Default Setting**

The default system priority is 1.

**Command Mode**

Global Configuration mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command configures the system priority to 120.

```
Console(config)# lacp system-priority 120
```
**lACP Commands**

**lacp port-priority**

The **lacp port-priority** Interface Configuration (Ethernet) mode command configures physical port priority. To return to the default configuration, use the **no** form of this command.

**Syntax**

```
lacp port-priority value
no lacp port-priority
```

**Parameters**

- **value** — Specifies port priority. (Range: 1 - 65535)

**Default Setting**

The default port priority is 1.

**Command Mode**

Interface Configuration (Ethernet) mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command defines the priority of Ethernet port 1/e6 as 247.

```
Console(config)# interface ethernet 1/e6
Console(config-if)# lacp port-priority 247
```
**lACP Commands**

**lacp timeout**

The `lacp timeout` Interface Configuration (Ethernet) mode command assigns an administrative LACP timeout. To return to the default configuration, use the `no` form of this command.

**Syntax**

`lacp timeout {long | short}`

`no lacp timeout`

**Parameters**

- **long** — Specifies the long timeout value.
- **short** — Specifies the short timeout value.

**Default Setting**

The default port timeout value is `long`.

**Command Mode**

Interface Configuration (Ethernet) mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command assigns a long administrative LACP timeout to Ethernet port 1/e6.

```
Console(config)# interface ethernet 1/e6
Console(config-if)# lacp timeout long
```
**show lACP ethernet**

The `show lACP ethernet` Privileged EXEC mode command displays LACP information for Ethernet ports.

**Syntax**

```
show lACP ethernet interface [parameters | statistics | protocol-state]
```

**Parameters**

- `interface` — Valid Ethernet port. (Full syntax: `port`)
- `parameters` — Link aggregation parameter information.
- `statistics` — Link aggregation statistics information.
- `protocol-state` — Link aggregation protocol-state information.

**Default Setting**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode

**Command Usage**

All LACP statistics is shown if no keyword is specified.

LACP should be enabled for selected Ethernet port.

**Example**

The following command displays LACP information for Ethernet port 1/e1.

```
Console# show lACP ethernet 1/e1
Port 1/e1 LACP parameters:
  Actor
  system priority: 1
  system mac addr: 00:00:12:34:56:78
  port Admin key: 30
  port Oper key: 30
  port Oper number: 21
  port Admin priority: 1
  port Oper priority: 1
  port Admin timeout: LONG
  port Oper timeout: LONG
  LACP Activity: ACTIVE
  Aggregation: AGGREGATABLE
  synchronization: FALSE
  collecting: FALSE
```
<table>
<thead>
<tr>
<th>Partner</th>
</tr>
</thead>
<tbody>
<tr>
<td>system priority: 0</td>
</tr>
<tr>
<td>system mac addr: 00:00:00:00:00:00</td>
</tr>
<tr>
<td>port Admin key: 0</td>
</tr>
<tr>
<td>port Oper key: 0</td>
</tr>
<tr>
<td>port Oper number: 0</td>
</tr>
<tr>
<td>port Admin priority: 0</td>
</tr>
<tr>
<td>port Oper priority: 0</td>
</tr>
<tr>
<td>port Oper timeout: LONG</td>
</tr>
<tr>
<td>LACP Activity: PASSIVE</td>
</tr>
<tr>
<td>Aggregation: AGGREGATABLE</td>
</tr>
<tr>
<td>synchronization: FALSE</td>
</tr>
<tr>
<td>collecting: FALSE</td>
</tr>
<tr>
<td>distributing: FALSE</td>
</tr>
<tr>
<td>expired: FALSE</td>
</tr>
</tbody>
</table>

Port 1/e1 LACP Statistics:
LACP PDUs sent: 2
LACP PDUs received: 2

Port 1/e1 LACP Protocol State:
LACP State Machines:
Receive FSM: Port Disabled State
Mux FSM: Detached State
Periodic Tx FSM: No Periodic State

Control Variables:
BEGIN: FALSE
LACP_ENABLED: TRUE
Ready_N: FALSE
Selected: UNSELECTED
Port_moved: FALSE
NNT: FALSE
Port_enabled: FALSE

Timer counters:
periodic tx timer: 0
current while timer: 0
wait while timer: 0
**show lACP port-channel**

The `show lACP port-channel` Privileged EXEC mode command displays LACP information for a port-channel.

**Syntax**

`show lACP port-channel [port_channel_number]`

**Parameters**

- `port_channel_number` — Valid port-channel number.

**Default Setting**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command displays LACP information about port-channel 1.

```
Console# show lACP port-channel 1
Port-Channel 1: Port Type 1000 Ethernet
    Actor
        System Priority: 1
        MAC Address: 00:02:85:0E:1C:00
        Admin Key: 29
        Oper Key: 29
    Partner
        System Priority: 0
        MAC Address: 00:00:00:00:00:00
        Oper Key: 14
```
Line Commands

**line**

The `line` Global Configuration mode command identifies a specific line for configuration and enters the Line Configuration command mode.

**Syntax**

```
line {console | telnet | ssh}
```

**Parameters**

- **console** — Console terminal line.
- **telnet** — Virtual terminal for remote console access (Telnet).
- **ssh** — Virtual terminal for secured remote console access (SSH).

**Default Setting**

This command has no default configuration.

**Command Mode**

Global Configuration mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command configures the device as a virtual terminal for remote console access.

```
Console(config)# line telnet
Console(config-line)#
```
speed

The **speed** Line Configuration mode command sets the line baud rate. To return to the default configuration, use the **no** form of the command.

**Syntax**

```
speed bps
no speed
```

**Parameters**

- `bps` — Baud rate in bits per second (bps). Possible values are 2400, 9600, 19200, 38400, 57600 and 115200.

**Default Setting**

The default speed is 9600 bps.

**Command Mode**

Line Configuration (console) mode

**Command Usage**

This command is available only on the line console.

The configured speed is applied when Autobaud is disabled. This configuration applies only to the current session.

**Example**

The following command configures the line baud rate to 115200.

```
Console(config)# line console
Console(config-line)# speed 115200
```
autobaud

The **autobaud** Line Configuration mode command sets the line for automatic baud rate detection (autobaud). To disable automatic baud rate detection, use the **no** form of the command.

**Syntax**

autobaud

no autobaud

**Parameters**

There are no parameters for this command.

**Default Setting**

Autobaud is disabled.

**Command Mode**

Line Configuration (console) mode

**Command Usage**

This command is available only on the line console.

To start communication using Autobaud, press <Enter> twice. This configuration applies only to the current session.

**Example**

The following command enables autobaud.

```
Console(config)# line console
Console(config-line)# autobaud
```
**exec-timeout**

The `exec-timeout` Line Configuration mode command sets the interval that the system waits until user input is detected. To return to the default configuration, use the `no` form of this command.

**Syntax**

```plaintext
exec-timeout minutes [seconds]
no exec-timeout
```

**Parameters**

- `minutes` — Specifies the number of minutes. (Range: 0-65535)
- `seconds` — Specifies additional time intervals in seconds. (Range: 0-59)

**Default Setting**

The default configuration is 10 minutes.

**Command Mode**

Line Configuration mode

**Command Usage**

To specify no timeout, enter the `exec-timeout 0` command.

**Example**

The following command configures the interval that the system waits until user input is detected to 20 minutes.

```plaintext
Console(config)# line console
Console(config-line)# exec-timeout 20
```
history

The `history` Line Configuration mode command enables the command history function. To disable the command history function, use the `no` form of this command.

**Syntax**

```
history
no history
```

**Parameters**

There are no parameters for this command.

**Default Setting**

The command history function is enabled.

**Command Mode**

Line Configuration mode

**Command Usage**

This command enables the command history function for a specified line. To enable or disable the command history function for the current terminal session, use the `terminal history` User EXEC mode command.

**Example**

The following command enables the command history function for telnet.

```
Console(config)# line telnet
Console(config-line)# history
```
**history size**

The **history size** Line Configuration mode command configures the command history buffer size for a particular line. To reset the command history buffer size to the default configuration, use the **no** form of this command.

**Syntax**

```
history size number-of-commands
no history size
```

**Parameters**

- **number-of-commands** — Number of commands that the system records in its history buffer.
  (Range: 10-216)

**Default Setting**

The default history buffer size is 10.

**Command Mode**

Line Configuration mode

**Command Usage**

This command configures the command history buffer size for a particular line. To configure the command history buffer size for the current terminal session, use the **terminal history size** User EXEC mode command. The maximum number of commands in all buffers is 256.

**Example**

The following command changes the command history buffer size to 100 entries for a particular line.

```
Console(config-line)# history size 100
```
terminal history

The terminal history user EXEC command enables the command history function for the current terminal session. To disable the command history function, use the no form of this command.

Syntax
terminal history
terminal no history

Parameters
There are no parameters for this command.

Default Setting
The default configuration for all terminal sessions is defined by the history line configuration command.

Command Mode
User EXEC mode

Command Usage
There are no user guidelines for this command.

Example
The following command disables the command history function for the current terminal session.

```
Console# no terminal history
```
**terminal history size**

The **terminal history size** User EXEC command configures the command history buffer size for the current terminal session. To reset the command history buffer size to the default setting, use the `no` form of this command.

**Syntax**

```
terminal history size number-of-commands
terminal no history size
```

**Parameters**

- `number-of-commands` — Specifies the number of commands the system may record in its command history buffer. (Range: 10-216)

**Default Setting**

The default history size for all terminal sessions is defined by the **history size** line configuration command.

**Command Mode**

User EXEC mode

**Command Usage**

The **terminal history size** user EXEC command configures the size of the command history buffer for the current terminal session. To change the default size of the command history buffer, use the **history** line configuration command.

The maximum number of commands in all buffers is 256.

**Example**

The following command configures the command history buffer size to 20 commands for the current terminal session.

```
Console# terminal history size 20
```
show line

The show line User EXEC mode command displays line parameters.

Syntax

show line [console | telnet | ssh]

Parameters

- **console** — Console terminal line.
- **telnet** — Virtual terminal for remote console access (Telnet).
- **ssh** — Virtual terminal for secured remote console access (SSH).

Default Setting

This command has no default configuration.

Command Mode

User EXEC mode

Command Usage

If line is not specified information for all lines is given.

Example

The following command displays the line configuration.

```
Console> show line

Console configuration:
Interactive timeout: Disabled
History: 10
Baudrate: 9600
Databits: 8
Parity: none
Stopbits: 1

Telnet configuration:
Interactive timeout: 10 minutes 10 seconds
History: 10

SSH configuration:
Interactive timeout: 10 minutes 10 seconds
History: 10
```
management access-list

The management access-list Global Configuration mode command configures a management access list and enters the Management Access-list Configuration command mode. To delete an access list, use the no form of this command.

Syntax
management access-list name
no management access-list name

Parameters
- name — Access list name. (Range: 1-32 characters)

Default Setting
This command has no default configuration.

Command Mode
Global Configuration mode

Command Usage
Use this command to configure a management access list. The command enters the Access-list Configuration mode, where permit and deny access rules are defined using the permit (Management) and deny (Management) commands.

If no match criteria are defined, the default is deny.

If you reenter an access list context, the new rules are entered at the end of the access list.

Use the management access-class command to select the active access list.

The active management list cannot be updated or removed.

Management ACL requires a valid management interface, which is a port, VLAN, or port-channel with an IP address or console interface. Management ACL only restricts access to the device for management configuration or viewing.
### Example

The following commands create a management access list called mlist, configure management Ethernet interfaces 1/e1 and 2/e9 and make the new access list the active list.

<table>
<thead>
<tr>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Console(config)# management access-list mlist</code></td>
</tr>
<tr>
<td><code>Console(config-macl)# permit ethernet 1/e1</code></td>
</tr>
<tr>
<td><code>Console(config-macl)# permit ethernet 2/e9</code></td>
</tr>
<tr>
<td><code>Console(config-macl)# exit</code></td>
</tr>
<tr>
<td><code>Console(config)# management access-class mlist</code></td>
</tr>
</tbody>
</table>

The following commands create a management access list called mlist, configure all interfaces to be management interfaces except Ethernet interfaces 1/e1 and 2/e9 and make the new access list the active list.

<table>
<thead>
<tr>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Console(config)# management access-list mlist</code></td>
</tr>
<tr>
<td><code>Console(config-macl)# deny ethernet 1/e1</code></td>
</tr>
<tr>
<td><code>Console(config-macl)# deny ethernet 2/e9</code></td>
</tr>
<tr>
<td><code>Console(config-macl)# permit</code></td>
</tr>
<tr>
<td><code>Console(config-macl)# exit</code></td>
</tr>
<tr>
<td><code>Console(config)# management access-class mlist</code></td>
</tr>
</tbody>
</table>
permit (Management)

The permit Management Access-List Configuration mode command defines a permit rule.

Syntax

```
permit [ethernet interface-number | vlan vlan-id | port-channel port-channel-number] [service service]
permit ip-source ip-address [mask mask | prefix-length] [ethernet interface-number | vlan vlan-id | port-channel port-channel-number] [service service]
```

Parameters

- `interface-number` — A valid Ethernet port number.
- `vlan-id` — A valid VLAN number.
- `port-channel-number` — A valid port channel index.
- `ip-address` — A valid source IP address.
- `mask` — A valid network mask of the source IP address.
- `prefix-length` — Number of bits that comprise the source IP address prefix. The prefix length must be preceded by a forward slash (/). (Range: 0-32)

Default Setting

If no permit rule is defined, the default is set to deny.

Command Mode

Management Access-list Configuration mode

Command Usage

Rules with Ethernet, VLAN and port-channel parameters are valid only if an IP address is defined on the appropriate interface.

The system supports up to 128 management access rules.

Example

The following command permits all ports in the mlist access list.

```
Console(config)# management access-list mlist
Console(config-macl)# permit
```
deny (Management)

The deny Management Access-List Configuration mode command defines a deny rule.

Syntax

deny [ethernet interface-number | vlan vlan-id | port-channel port-channel-number] [service service]
deny ip-source ip-address [mask mask | prefix-length] [ethernet interface-number | vlan vlan-id | port-channel port-channel-number | ] [service service]

Parameters

■ interface-number — A valid Ethernet port number.
■ vlan-id — A valid VLAN number.
■ port-channel-number — A valid port-channel number.
■ ip-address — A valid source IP address.
■ mask — A valid network mask of the source IP address.
■ prefix-length — Specifies the number of bits that comprise the source IP address prefix. The prefix length must be preceded by a forward slash (/). (Range: 0-32)

Default Setting

This command has no default configuration.

Command Mode

Management Access-list Configuration mode

Command Usage

Rules with Ethernet, VLAN and port-channel parameters are valid only if an IP address is defined on the appropriate interface.

The system supports up to 128 management access rules.

Example

The following command denies all ports in the access list called mlist.

```
Console(config)# management access-list mlist
Console(config-macl)# deny
```
management access-class

The **management access-class** Global Configuration mode command restricts management connections by defining the active management access list. To disable this restriction, use the **no** form of this command.

**Syntax**

management access-class {console-only | name}

no management access-class

**Parameters**

- **console-only** — Indicates that the device can be managed only from the console.
- **name** — Specifies the name of the access list to be used. (Range: 1-32 characters)

**Default Setting**

No active management access list specified.

**Command Mode**

Global Configuration mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command configures an access list called *mlist* as the management access list.

```
Console(config)# management access-class mlist
```
**show management access-list**

The `show management access-list` Privileged EXEC mode command displays management access-lists.

**Syntax**

```
show management access-list [name]
```

**Parameters**

- `name` — Specifies the name of a management access list. (Range: 1-32 characters)

**Default Setting**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command displays the mlist management access list.

```
Console# show management access-list mlist
mlist
-----
    permit ethernet 1/e1
    permit ethernet 2/e2
! (Note: all other access implicitly denied)
```
show management access-class

The show management access-class Privileged EXEC mode command displays the active management access list.

Syntax
show management access-class

Parameters
There are no parameters for this command.

Default Setting
This command has no default configuration.

Command Mode
Privileged EXEC mode

Command Usage
There are no user guidelines for this command.

Example
The following command displays information about the active management access list.

```
Console# show management access-class
Management access-class is enabled, using access list mlist
```
Management ACL Commands
PHY Diagnostics Commands

**test copper-port tdr**

The `test copper-port tdr` Privileged EXEC mode command uses Time Domain Reflectometry (TDR) technology to diagnose the quality and characteristics of a copper cable attached to a port.

**Syntax**

`test copper-port tdr interface`

**Parameters**

- `interface` — A valid Ethernet port. (Full syntax: `port`)

**Default Setting**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode

**Command Usage**

The port to be tested should be shut down during the test, unless it is a combination port with the fiber port active.

The maximum length of the cable for the TDR test is 120 meters.

**Example**

The following command results in a report on the cable attached to port 1/e3.

```
Console# test copper-port tdr 1/e3
Cable is open at 64 meters

Console# test copper-port tdr 2/g1
Can't perform this test on fiber ports
```
**show copper-ports tdr**

The **show copper-ports tdr** User EXEC mode command displays information on the last Time Domain Reflectometry (TDR) test performed on copper ports.

**Syntax**

```
show copper-ports tdr [interface]
```

**Parameters**

- **interface** — A valid Ethernet port. (Full syntax: port)

**Default Setting**

This command has no default configuration.

**Command Mode**

User EXEC mode

**Command Usage**

The maximum length of the cable for the TDR test is 120 meters.

**Example**

The following command displays information on the last TDR test performed on all copper ports.

```
Console> show copper-ports tdr

Port  Result  Length [meters]  Date
-----  ------  --------------- ----
 1/e1   OK     -  -
 1/e2   Short  50  13:32:00 23 July 2005
 1/e3  Test has not been performed
 1/e4   Open  64  13:32:00 23 July 2005
 1/g1   Fiber- -  -
```
show copper-ports cable-length

The `show copper-ports cable-length` User EXEC mode command displays the estimated copper cable length attached to a port.

**Syntax**

`show copper-ports cable-length [interface]`

**Parameters**

- `interface` — A valid Ethernet port. (Full syntax: `port`)

**Default Setting**

This command has no default configuration.

**Command Mode**

User EXEC mode

**Command Usage**

The port must be active and working in 100M or 1000M mode.

**Example**

The following command displays the estimated copper cable length attached to all ports.

```
Console> show copper-ports cable-length

<table>
<thead>
<tr>
<th>Port</th>
<th>Length [meters]</th>
</tr>
</thead>
<tbody>
<tr>
<td>----</td>
<td>-------------------</td>
</tr>
<tr>
<td>1/e1</td>
<td>&lt; 50</td>
</tr>
<tr>
<td>1/e2</td>
<td>Copper not active</td>
</tr>
<tr>
<td>1/e3</td>
<td>110-140</td>
</tr>
<tr>
<td>1/g1</td>
<td>Fiber</td>
</tr>
</tbody>
</table>
```
show fiber-ports optical-transceiver

The `show fiber-ports optical-transceiver` Privileged EXEC command displays the optical transceiver diagnostics.

**Syntax**

`show fiber-ports optical-transceiver [interface] [detailed]`

**Parameters**

- `interface` — A valid Ethernet port. (Full syntax: `port`)
- `detailed` — Detailed diagnostics.

**Default Setting**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode

**Command Usage**

To test optical transceivers, ensure a fiber link is present.

**Examples**

The following commands display the optical transceiver diagnostics.

<table>
<thead>
<tr>
<th>Port</th>
<th>Temp</th>
<th>Voltage</th>
<th>Current</th>
<th>Output</th>
<th>Input</th>
<th>TX Fault</th>
<th>LOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/g1</td>
<td>W</td>
<td>OK</td>
<td>E</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
</tr>
<tr>
<td>1/g2</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
<td>E</td>
<td>OK</td>
</tr>
<tr>
<td>1/g3</td>
<td>Copper</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Temp – Internally measured transceiver temperature.
Voltage - Internally measured supply voltage.
Current – Measured TX bias current.
Output Power – Measured TX output power.
Input Power – Measured RX received power.
Tx Fault – Transmitter fault
LOS – Loss of signal
N/A - Not Available, N/S - Not Supported, W - Warning, E - Error
### PHY Diagnostics Commands

#### Console# **show fiber-ports optical-transceiver detailed**

<table>
<thead>
<tr>
<th>Port</th>
<th>Temp</th>
<th>Voltage</th>
<th>Current</th>
<th>Output</th>
<th>Input</th>
<th>TX Fault</th>
<th>LOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/g1</td>
<td>48</td>
<td>5.15</td>
<td>50</td>
<td>1.789</td>
<td>1.789</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>1/g2</td>
<td>43</td>
<td>5.15</td>
<td>10</td>
<td>1.789</td>
<td>1.789</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>1/g3</td>
<td>Copper</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Temp – Internally measured transceiver temperature.

Voltage - Internally measured supply voltage.

Current – Measured TX bias current.

Output Power – Measured TX output power.

Input Power – Measured RX received power.

Tx Fault – Transmitter fault

LOS – Loss of signal
interface port-channel

The **interface port-channel** Global Configuration mode command enters the interface configuration mode to configure a specific port-channel.

**Syntax**

```
interface port-channel port-channel-number
```

**Parameters**

- `port-channel-number` — A valid port-channel number.

**Default Setting**

This command has no default configuration.

**Command Mode**

Global Configuration mode

**Command Usage**

Eight aggregated links can be defined with up to eight member ports per port-channel. The aggregated links’ valid IDs are 1-8.

**Example**

The following command enters the context of port-channel number 1.

```
Console(config)# interface port-channel 1
```
interface range port-channel

The interface range port-channel Global Configuration mode command enters the interface configuration mode to configure multiple port-channels.

Syntax

interface range port-channel {port-channel-range \ all}

Parameters

- port-channel-range — List of valid port-channels to add. Separate nonconsecutive port-channels with a comma and no spaces. A hyphen designates a range of port-channels.
- all — All valid port-channels.

Default Setting

This command has no default configuration.

Command Mode

Global Configuration mode

Command Usage

Commands under the interface range context are executed independently on each interface in the range.

Example

In the following example, port-channels 1, 2 and 6 are grouped to receive the same command.

```
Console(config)# interface range port-channel 1-2,6
```
channel-group

The channel-group Interface Configuration (Ethernet) mode command associates a port with a port-channel. To remove a port from a port-channel, use the no form of this command.

Syntax

channel-group port-channel-number mode {on | auto}
no channel-group

Parameters

- **port-channel_number** — Specifies the ID of the valid port-channel for the current port to join.
- **on** — Forces the port to join a channel without an LACP operation.
- **auto** — Allows the port to join a channel as a result of an LACP operation.

Default Setting

The port is not assigned to a port-channel.

Command Mode

Interface Configuration (Ethernet) mode

Command Usage

There are no user guidelines for this command.

Example

The following command forces port 1/e1 to join port-channel 1 without an LACP operation.

```
Console(config)# interface ethernet 1/e1
Console(config-if)# channel-group 1 mode on
```
show interfaces port-channel

The `show interfaces port-channel` Privileged EXEC mode command displays port-channel information.

**Syntax**

`show interfaces port-channel [port-channel-number]`

**Parameters**

- `port-channel-number` — Valid port-channel number.

**Default Setting**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command displays information on all port-channels.

```
Console# show interfaces port-channel

<table>
<thead>
<tr>
<th>Channel</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Active: 1/e1, 2/e2</td>
</tr>
<tr>
<td>2</td>
<td>Active: 2/e2, 2/e7 Inactive: 3/e1</td>
</tr>
<tr>
<td>3</td>
<td>Active: 3/e3, 3/e8</td>
</tr>
</tbody>
</table>
```
Port Monitor Commands

port monitor

The port monitor Interface Configuration mode command starts a port monitoring session. To stop a port monitoring session, use the no form of this command.

Syntax

port monitor src-interface [rx | tx]
no port monitor src-interface

Parameters

- src-interface — Valid Ethernet port. (Full syntax: port)
- rx — Monitors received packets only.
- tx — Monitors transmitted packets only.

Default Setting

Monitors both received and transmitted packets. No port monitors are configured by default.

Command Mode

Interface Configuration (Ethernet) mode

Command Usage

This command enables traffic on one port to be copied to another port, or between the source port (src-interface) and a destination port (port being configured).

The following restrictions apply to ports configured as destination ports:

- The port cannot be already configured as a source port.
- The port cannot be a member in a port-channel.
- An IP interface is not configured on the port.
- GVRP is not enabled on the port.
- The port is not a member of a VLAN, except for the default VLAN (will automatically be removed from the default VLAN).

The following restrictions apply to ports configured to be source ports:

- The port cannot be already configured as a destination port.
Example

The following command copies traffic on port 1/e8 (source port) to port 1/e1 (destination port).

```
Console(config)# interface ethernet 1/e1
Console(config-if)# port monitor 1/e8
```
show ports monitor

The `show ports monitor` User EXEC mode command displays the port monitoring status.

**Syntax**

`show ports monitor`

**Parameters**

There are no parameters for this command.

**Default Setting**

This command has no default configuration.

**Command Mode**

User EXEC mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command displays the port monitoring status.

```
Console> show ports monitor

<table>
<thead>
<tr>
<th>Source Port</th>
<th>Destination Port</th>
<th>Type</th>
<th>Status</th>
<th>VLAN Tagging</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/e1</td>
<td>1/e8</td>
<td>RX,TX</td>
<td>Active</td>
<td>No</td>
</tr>
<tr>
<td>1/e2</td>
<td>1/e8</td>
<td>RX,TX</td>
<td>Active</td>
<td>No</td>
</tr>
<tr>
<td>1/e18</td>
<td>1/e8</td>
<td>RX</td>
<td>Active</td>
<td>No</td>
</tr>
</tbody>
</table>
```
The `qos` Global Configuration mode command enables Quality of Service (QoS) on the device. To disable QoS on the device, use the `no` form of this command.

**Syntax**

```
qos [basic | advanced]
no qos
```

**Parameters**

- **basic** — QoS basic mode. **This mode is applied if no keyword is specified.**
- **advanced** — QoS advanced mode, which enables the full range of QoS configuration.

**Default Setting**

The QoS basic mode is enabled.

**Command Mode**

Global Configuration mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command enables QoS on the device.

```
Console(config)# qos
```
show qos

The show qos User EXEC mode command displays the quality of service (QoS) mode for the device.

Syntax
show qos

Parameters
There are no parameters for this command.

Default Setting
This command has no default configuration.

Command Mode
User EXEC mode

Command Usage
Trust mode is displayed if QoS is enabled in basic mode.

Example
The following command displays QoS attributes when QoS is enabled in basic mode on the device.

```
Console> show qos
Qos: basic
Basic trust: dscp
```
class-map

The create-map Global Configuration mode command creates or modifies a class map and enters the Class-map Configuration mode. To delete a class map, use the no form of this command.

Syntax

```plaintext
class-map class-map-name [match-all | match-any]
no class-map class-map-name
```

Parameters

- `class-map-name` — Specifies the name of the class map.
- `match-all` — Checks that the packet matches all classification criteria in the class map match statement (Logical AND for selected ACLs).
- `match-any` — Checks that the packet matches one or more classification criteria in the class map match statement (Logical OR for selected ACLs).

Default Setting

By default, the `match-all` parameter is selected.

Command Mode

Global Configuration mode

Command Usage

The class-map Global Configuration mode command is used to define packet classification, marking and aggregate policing as part of a globally named service policy applied on a per-interface basis.

The Class-Map Configuration mode enables entering up to two match Class-map Configuration mode commands to configure the classification criteria for the specified class. If two match Class-map Configuration mode commands are entered, each should point to a different type of ACL (e.g., one to an IP ACL and one to a MAC ACL). Since packet classification is based on the order of the classification criteria, the order in which the match Class-Map Configuration mode commands are entered is important.

If there is more than one match statement in a match-all class map and the same classification field appears in the participating ACLs, an error message is generated.

Note the following:

- A class map in match-all mode cannot be configured if it contains both an IP ACL and a MAC ACL with an ether type that is not 0x0800.
- Class map can be defined only in QoS Advanced mode.
**Example**

The following command creates a class map called class1 and configures it to check that packets match all classification criteria in the class map match statement.

```
Console(config)# class-map class1 match-all
Console(config-cmap)#
```
**show class-map**

The `show class-map` User EXEC mode command displays all class maps.

**Syntax**

```
show class-map [class-map-name]
```

**Parameters**

- `class-map-name` — Specifies the name of the class map to be displayed.

**Default Setting**

This command has no default configuration.

**Command Mode**

User EXEC mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command shows the class map for class1.

```
Console> show class-map class1
Class Map match-any class1 (id4)
Match ip dscp 11 21
```
**match**

The **match** Class-map Configuration mode command defines the match criteria for classifying traffic. To delete the match criteria, use the **no** form of this command.

**Syntax**

```plaintext
match access-group acl-name
no match access-group acl-name
```

**Parameters**

- **acl-name** — Specifies the name of an IP or MAC ACL.

**Default Setting**

No match criterion is supported.

**Command Mode**

Class-map Configuration mode.

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command defines the match criterion for classifying traffic as an access group called HP in a class map called class1.

```
Console(config)# class-map class1
Console(config-cmap)# match access-group hp
```
**policy-map**

The **policy-map** Global Configuration mode command creates a policy map and enters the Policy-map Configuration mode. To delete a policy map, use the **no** form of this command.

**Syntax**

```
policy-map policy-map-name
no policy-map policy-map-name
```

**Parameters**

- `policy-map-name` — Specifies the name of the policy map.

**Default Setting**

If the packet is an IP packet, the DCSP value of the policy map is 0.
If the packet is tagged, the CoS value is 0.

**Command Mode**

Global Configuration mode

**Command Usage**

Before configuring policies for classes whose match criteria are defined in a class map, use the **policy-map** Global Configuration mode command to specify the name of the policy map to be created or modified.

Class policies in a policy map can only be defined if match criteria has already been defined for the classes. Use the **class-map** Global Configuration and **match** Class-map Configuration commands to define the match criteria of a class.

Only one policy map per interface per direction is supported. A policy map can be applied to multiple interfaces and directions.

**Example**

The following command creates a policy map called policy1 and enters the Policy-map Configuration mode.

```
Console (config)# policy-map policy1
Console (config-pmap)#
```


**class**

The `class` Policy-map Configuration mode command defines a traffic classification and enters the Policy-map Class Configuration mode. To remove a class map from the policy map, use the `no` form of this command.

**Syntax**

class class-map-name [access-group acl-name]
no class class-map-name

**Parameters**

- `class-map-name` — Specifies the name of an existing class map. If the class map does not exist, a new class map will be created under the specified name.
- `acl-name` — Specifies the name of an IP or MAC ACL.

**Default Setting**

No policy map is defined.

**Command Mode**

Policy-map Configuration mode

**Command Usage**

Before modifying a policy for an existing class or creating a policy for a new class, use the `policy-map` Global Configuration mode command to specify the name of the policy map to which the policy belongs and to enter the Policy-map Configuration mode.

Use the `service-policy` (Ethernet, Port-channel) Interface Configuration mode command to attach a policy map to an interface.

Use an existing class map to attach classification criteria to the specified policy map and use the `access-group` parameter to modify the classification criteria of the class map.

If this command is used to create a new class map, the name of an IP or MAC ACL must also be specified.

**Example**

The following command defines a traffic classification called class1 with an access-group called HP. The class is in a policy map called policy1.

```
Console(config)# policy-map policy1
Console (config-pmap)# class class1 access-group HP
```
**show policy-map**

The `show policy-map` User EXEC command displays the policy maps.

**Syntax**

```
show policy-map [policy-map-name [class class-name]]
```

**Parameters**

- **policy-map-name** — Specifies the name of the policy map to be displayed.
- **class-name** — Specifies the name of the class whose QoS policies are to be displayed.

**Default Setting**

This command has no default configuration.

**Command Mode**

User EXEC mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command displays all policy maps.

```
Console> show policy-map
Policy Map policy1
    class class1
        set lp dscp 7

Policy Map policy2
    class class 2
        police 96000 4800 exceed-action drop
        class class3
            police 124000 96000 exceed-action policed-dscp-transmit
```
**trust cos-dscp**

The `trust cos-dscp` Policy-map Class Configuration mode command configures the trust state. The trust state determines the source of the internal DSCP value used by Quality of Service (QoS). To return to the default configuration, use the `no` form of this command.

**Syntax**

```
trust cos-dscp
no trust cos-dscp
```

**Parameters**

There are no parameters for this command.

**Default Setting**

The port is not in the trust mode.

If the port is in trust mode, the internal DSCP value is derived from the ingress packet.

**Command Mode**

Policy-map Class Configuration mode

**Command Usage**

Action serviced to a class, so that if an IP packet arrives, the queue is assigned per DSCP. If a non-IP packet arrives, the queue is assigned per CoS (VPT).

**Example**

The following command configures the trust state for a class called class1 in a policy map called policy1.

```plaintext
Console (config)# policy-map policy1
Console (config-pmap)# class class1
Console (config-pmap-c)# trust cos-dscp
```
set

The set Policy-map Class Configuration mode command sets new values in the IP packet.

Syntax

set {dscp new-dscp | queue queue-id | cos new-cos}

no set

Parameters

■ new-dscp — Specifies a new DSCP value for the classified traffic. (Range: 0-63)
■ queue-id — Specifies an explicit queue ID for setting the egress queue.
■ new-cos — Specifies a new user priority for marking the packet. (Range: 0-7)

Default Setting

This command has no default configuration.

Command Mode

Policy-map Class Configuration mode

Command Usage

This command is mutually exclusive with the trust Policy-map Class Configuration command within the same policy map.

Policy maps that contain set or trust Policy-map Class Configuration commands or that have ACL classifications cannot be attached to an egress interface by using the service-policy (Ethernet, Port-channel) Interface Configuration mode command.

To return to the Policy-map Configuration mode, use the exit command. To return to privileged EXEC mode, use the end command.

Example

The following command sets the DSCP value in the packet to 56 for classes in in policy map called policy class map class1.

```
Console (config)# policy-map policy1
Console (config-pmap)# class class1
Console (config-pmap-c)# set dscp 56
```
**police**

The `police` Policy-map Class Configuration mode command defines the policer for classified traffic. To remove a policer, use the `no` form of this command.

**Syntax**

```plaintext
police committed-rate-bps committed-burst-byte [exceed-action {drop | policed-dscp-transmit}]
no police
```

**Parameters**

- `committed-rate-bps` — Specifies the average traffic rate (CIR) in bits per second (bps).
- `committed-burst-byte` — Specifies normal burst size (CBS) in bytes.
- `drop` — Indicates that when the rate is exceeded, the packet is dropped.
- `policed-dscp-transmit` — Indicates that when the rate is exceeded, the DSCP of the packet is remarked according to the policed-DSCP map as configured by the `qos map policed-dscp` Global Configuration mode command.

**Default Setting**

This command has no default configuration.

**Command Mode**

Policy-map Class Configuration mode

**Command Usage**

Policing uses a token bucket algorithm. CIR represents the speed with which the token is removed from the bucket. CBS represents the depth of the bucket.

Policy maps that contain `set` or `trust` Policy-map Class Configuration commands or that have ACL classifications cannot be attached to an egress interface by using the `service-policy` (Ethernet, Port-channel) Interface Configuration mode command.

**Example**

The following command defines a policer for classified traffic. When the traffic rate exceeds 124,000 bps or the normal burst size exceeds 96000 bytes, the packet is dropped. The class is called `class1` and is in a policy map called `policy1`.

```plaintext
Console (config)# policy-map policy1
Console (config-pmap)# class class1
Console (config-pmap-c)# police 124000 96000 exceed-action drop
```
service-policy

The service-policy Interface Configuration (Ethernet, port-channel) mode command applies a policy map to the input of a particular interface. To detach a policy map from an interface, use the no form of this command.

Syntax

service-policy {input policy-map-name}
no service-policy {input}

Parameters

- policy-map-name — Specifies the name of the policy map to be applied to the input interface.

Default Setting

This command has no default configuration.

Command Mode

Interface Configuration (Ethernet, port-Channel) mode

Command Usage

Only one policy map per interface per direction is supported.

Example

The following command attaches a policy map called policy1 to the input interface.

```console
Console(config-if)# service-policy input policy1
```
QoS Commands

qos aggregate-policer

The qos aggregate-policer Global Configuration mode command defines the policer parameters that can be applied to multiple traffic classes within the same policy map. To remove an existing aggregate policer, use the no form of this command.

Syntax

qos aggregate-policer aggregate-policer-name committed-rate-bps excess-burst-byte exceed-action {drop | policed-dscp-transmit} [dscp dscp]

no qos aggregate-policer

Parameters

- aggregate-policer-name — Specifies the name of the aggregate policer.
- committed-rate-bps — Specifies the average traffic rate (CIR) in bits per second (bps).
- excess-burst-byte — Specifies the normal burst size (CBS) in bytes.
- drop — Indicates that when the rate is exceeded, the packet is dropped.
- policed-dscp-transmit — Indicates that when the rate is exceeded, the DSCP of the packet is remarked.
- dscp — Specifies the value that the DSCP would be remarked. If unspecified, the DSCP would be remarked according to the policed-DSCP map as configured by the qos map policed-dscp Global Configuration mode command.

Default Setting

No aggregate policer is define.

Command Mode

Global Configuration mode

Command Usage

Define an aggregate policer if the policer is shared with multiple classes.

Policers in one port cannot be shared with other policers in another device; traffic from two different ports can be aggregated for policing purposes.

An aggregate policer can be applied to multiple classes in the same policy map; An aggregate policer cannot be applied across multiple policy maps.

An aggregate policer cannot be deleted if it is being used in a policy map. The no police aggregate Policy-map Class Configuration command must first be used to delete the aggregate policer from all policy maps.

Policing uses a token bucket algorithm. CIR represents the speed with which the token is removed from the bucket. CBS represents the depth of the bucket.

Example

The following command defines the parameters of an aggregate policer called policer1 that can be applied to multiple classes in the same policy map. When the average traffic rate exceeds 124,000 bps or the normal burst size exceeds 96000 bytes, the packet is dropped.

Console (config)# qos aggregate-policer policer1 124000 96000 exceed-action drop
show qos aggregate-policer

The `show qos aggregate-policer` User EXEC mode command displays the aggregate policer parameter.

**Syntax**

```plaintext
show qos aggregate-policer [aggregate-policer-name]
```

**Parameters**

- `aggregate-policer-name` — Specifies the name of the aggregate policer to be displayed.

**Default Setting**

This command has no default configuration.

**Command Mode**

User EXEC mode

**Command Usage**

There are no user guidelines.

**Example**

The following command displays the parameters of the aggregate policer called policer1.

```
Console> show qos aggregate-policer policer1
aggregate-policer policer1 96000 4800 exceed-action drop
not used by any policy map
```
police aggregate

The `police aggregate` Policy-map Class Configuration mode command applies an aggregate policer to multiple classes within the same policy map. To remove an existing aggregate policer from a policy map, use the `no` form of this command.

**Syntax**

`police aggregate aggregate-policer-name`

`no police aggregate aggregate-policer-name`

**Parameters**

- `aggregate-policer-name` — Specifies the name of the aggregate policer.

**Default Setting**

This command has no default configuration.

**Command Mode**

Policy-map Class Configuration mode

**Command Usage**

An aggregate policer can be applied to multiple classes in the same policy map; An aggregate policer cannot be applied across multiple policy maps or interfaces.

To return to the Policy-map Configuration mode, use the `exit` command. To return to the Privileged EXEC mode, use the `end` command.

**Example**

The following command applies the aggregate policer called policer1 to a class called class1 in policy map called policy1.

```
Console(config)# policy-map policy1
Console(config-pmap)# class class1
Console(config-pmap-c)# police aggregate policer1
```
**wrr-queue cos-map**

The `wrr-queue cos-map` Global Configuration mode command maps Class of Service (CoS) values to a specific egress queue. To return to the default configuration, use the `no` form of this command.

**Syntax**

```
wrr-queue cos-map queue-id cos1...cos8
no wrr-queue cos-map [queue-id]
```

**Parameters**

- `queue-id` — Specifies the queue number to which the CoS values are mapped.
- `cos1...cos8` — Specifies CoS values to be mapped to a specific queue. (Range: 0-7)

**Default Setting**

Default cos to queue map

**Command Mode**

Global Configuration mode

**Command Usage**

This command can be used to distribute traffic into different queues, where each queue is configured with different Weighted Round Robin (WRR) and Weighted Random Early Detection (WRED) parameters.

It is recommended to specifically map a single VPT to a queue, rather than mapping multiple VPTs to a single queue. Use the `priority-queue out num-of-queues` Interface Configuration (Ethernet, Port-channel) mode command to enable expedite queues.

**Example**

The following command maps CoS 7 to queue 2.

```
Console(config)# wrr-queue cos-map 2 7
```
priority-queue out num-of-queues

The priority-queue out num-of-queues Global Configuration mode command configures the number of expedite queues. To return to the default configuration, use the no form of this command.

Syntax

priority-queue out num-of-queues number-of-queues
no priority-queue out num-of-queues

Parameters

- number-of-queues — Specifies the number of expedite queues. Expedite queues have higher indexes. (Range: 0-4)

Default Setting

All queues are expedite queues.

Command Mode

Global Configuration mode

Command Usage

Configuring the number of expedite queues affects the Weighted Round Robin (WRR) weight ratio because fewer queues participate in the WRR.

Example

The following command configures the number of expedite queues as 0.

```
Console(config)# priority-queue out num-of-queues 0
```
traffic-shape

The **traffic-shape** Interface Configuration (Ethernet, port-channel) mode command configures the shaper of the egress port/queue. To disable the shaper, use the **no** form of this command.

**Syntax**

```
traffic-shape { committed-rate committed-burst }
no traffic-shape
```

**Parameters**

- **committed-rate** — Specifies the average traffic rate (CIR) in bits per second (bps).
  
  (Range: 6510-1073741800)

- **excess-burst** — Specifies the excess burst size (CBS) in bytes.

**Default Setting**

No shape is defined.

**Command Mode**

Interface Configuration (Ethernet, port-channel) mode

**Command Usage**

This command activates the shaper on a specified egress port or egress queue.

Use the command with the “burst” parameter for GE ports, and without the “burst” parameter for FE ports.

To activate the shaper on an egress port, enter the Interface Configuration mode. Then run this command without the **queue-id** parameter. The CIR and the CBS will be applied to the specified port.

To activate the shaper for specific queue, run this command with the **queue-id** parameter.

**Example**

The following command sets a shaper on Ethernet port 1/g4 when the average traffic rate exceeds 124000 bps or the normal burst size exceeds 96000 bps.

```
Console(config)# interface ethernet 1/g4
Console(config-if)# traffic-shape 124000 96000
```
**show qos interface**

The `show qos interface` User EXEC mode command displays Quality of Service (QoS) information on the interface.

**Syntax**

```
show qos interface [ethernet interface-number | port-channel number] [buffers | queueing | policers | shapers]
```

**Parameters**

- `interface-number` — Valid Ethernet port number.
- `number` — Valid port-channel number.
- `buffers` — Displays the buffer setting for the interface’s queues. Displays the queue depth for each queue and the thresholds for the WRED.
- `queueing` — Displays the queue strategy (WRR or EF), the weight for WRR queues, the CoS to queue map and the EF priority.
- `policers` — Displays all the policers configured for this interface, their setting and the number of policers currently unused.
- `shapers` — Displays the shaper of the specified interface and the shaper for the queue on the specified interface.

**Default Setting**

There is no default configuration for this command.

**Command Mode**

User EXEC mode

**Command Usage**

If no keyword is specified, port QoS mode (e.g., DSCP trusted, CoS trusted, untrusted), default CoS value, DSCP-to-DSCP-mutation map attached to the port, and policy map attached to the interface are displayed.

If no interface is specified, QoS information about all interfaces is displayed.
Example

The following command displays the buffer settings for queues on Ethernet port 1/e1.

```
Console# show qos interface buffers ethernet e3
Ethernet e3
Port 3 wrong port type= 2

Notify Q depth:
qid - size
  1 - 300
  2 - 300
  3 - 300
  4 - 300

qid threshTMibScalarC_SetValue: var: rlIfProfileName mismatching between var mib type and object type!
  1 0
TMibScalarC_SetValue: var: rlIfProfileName mismatching between var mib type and object type!
  2 0
TMibScalarC_SetValue: var: rlIfProfileName mismatching between var mib type and object type!
  3 0
TMibScalarC_SetValue: var: rlIfProfileName mismatching between var mib type and object type!
  4 0

qid WRED thresh0 thresh1 thresh2
TMibScalarC_SetValue: var: rlIfProfileName mismatching between var mib type and object type!
  1 disable 0 0 0
TMibScalarC_SetValue: var: rlIfProfileName mismatching between var mib type and object type!
  2 disable 0 0 0
TMibScalarC_SetValue: var: rlIfProfileName mismatching between var mib type and object type!
  3 disable 0 0 0
TMibScalarC_SetValue: var: rlIfProfileName mismatching between var mib type and object type!
  4 disable 0 0 0

qid MinDP0 MaxDP0 ProbDP0 MinDP1 MaxDP1 ProbDP1 MinDP2 MaxDP2 ProbDP2 weight
TMibScalarC_SetValue: var: rlIfProfileName mismatching between var mib type and object type!
  1 N/A N/A N/A N/A N/A N/A N/A N/A N/A N/A N/A
TMibScalarC_SetValue: var: rlIfProfileName mismatching between var mib type and object type!
  2 N/A N/A N/A N/A N/A N/A N/A N/A N/A N/A N/A
TMibScalarC_SetValue: var: rlIfProfileName mismatching between var mib type and object type!
  3 N/A N/A N/A N/A N/A N/A N/A N/A N/A N/A N/A
TMibScalarC_SetValue: var: rlIfProfileName mismatching between var mib type and object type!
  4 N/A N/A N/A N/A N/A N/A N/A N/A N/A N/A N/A

Console#
```
**wrr-queue threshold**

The **wrr-queue threshold** Global Configuration mode command assigns queue thresholds globally. To return to the default configuration, use the no form of this command.

**Syntax**

```
qos wrr-queue threshold gigabitethernet queue-id threshold-percentage
no qos wrr-queue threshold gigabitethernet queue-id
no qos wrr-queue threshold tengigabitethernet queue-id
```

**Parameters**

- `gigabitethernet` — Indicates that the thresholds are to be applied to Gigabit Ethernet ports.
- `queue-id` — Specifies the queue number to which the threshold is assigned.
- `threshold-percentage 0,1,2` — Specifies the queue threshold percentage value. Each value is separated by a space. (Range: 0-100)

**Default Setting**

80 percent for all thresholds.

**Command Mode**

Global Configuration mode.

**Command Usage**

The packet refers to a certain threshold by the conformance level. If threshold 0 is exceeded, packets with the corresponding DP (Drop Precedence) are dropped until the threshold is no longer exceeded. However, packets assigned to threshold 1 or 2 continue to be queued and sent as long as the second or third threshold is not exceeded.

**Example**

The following command assigns a threshold of 80 percent to WRR queue 1.

```
Console (config)# qos wrr-queue threshold gigabitethernet 1
```
**qos map dscp-dp**

The `qos map dscp-dp` global configuration mode command maps DSCP to Drop Precedence. To return to the default setting, use the `no` form of this command.

**Syntax**

```
qos map dscp-dp dscp-list to dp
no qos map dscp-dp
```

**Parameters**

- `dscp-list` — Specifies up to 8 DSCP values separated by a space (Range: 0-63).
- `dp` — Enter the Drop Precedence value to which the DSCP value corresponds.
  (Possible values are 0 - 2 where 2 is the highest Drop Precedence)

**Default Setting**

All the DSCPs are mapped to Drop Precedence 0.

**Command Mode**

Global Configuration mode.

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command maps DSCP to Drop Precedence.

```
console (config) # qos map dscp-dp 0 to 63
```
qos map policed-dscp

The `qos map policed-dscp` Global Configuration mode command modifies the policed-DSCP map for remarking purposes. To return to the default map, use the `no` form of this command.

**Syntax**

`qos map policed-dscp dscp-list to dscp-mark-down`

`no qos map policed-dscp`

**Parameters**

- `dscp-list` — Specifies up to 8 DSCP values separated by a space. (Range: 0-63)
- `dscp-mark-down` — Specifies the DSCP value to mark down. (Range: 0-63)

**Default Setting**

The default map is the Null map, which means that each incoming DSCP value is mapped to the same DSCP value.

**Command Mode**

Global Configuration mode.

**Command Usage**

DSCP values 3,11,19… cannot be remapped to other values. The mapping of the IP DSCP to priority queue is set on a per system basis. If this mode is active, a non-IP packet is always classified to the best effort queue.

**Example**

The following command fails to mark down incoming DSCP value 3 as DSCP value 43 on the policed-DSCP map.

```
Console(config)# qos map policed-dscp 3 to 43
Reserved DSCP. DSCP 3 was not configured.
```
**qos map dscp-queue**

The **qos map dscp-queue** Global Configuration mode command modifies the DSCP to CoS map. To return to the default map, use the **no** form of this command.

**Syntax**

```
qos map dscp-queue dscp-list to queue-id
no qos map dscp-queue
```

**Parameters**

- **dscp-list** — Specifies up to 8 DSCP values separated by a space. (Range: 0-63)
- **queue-id** — Specifies the queue number to which the DSCP values are mapped.

**Default Setting**

The following table describes the default map.

<table>
<thead>
<tr>
<th>DSCP Value</th>
<th>Queue Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-15</td>
<td>q1 (Lowest Priority)</td>
</tr>
<tr>
<td>16-31</td>
<td>q2</td>
</tr>
<tr>
<td>32-47</td>
<td>q3</td>
</tr>
<tr>
<td>48-63</td>
<td>q4</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command maps DSCP values 33, 40 and 41 to queue 1.

```
Console(config)# qos map dscp-queue 33 40 41 to 1
```
qos trust (Global)

The **qos trust** Global Configuration mode command configures the system to the basic mode and trust state. To return to default state (trust VPT), use the **no** form of the command.

**Syntax**

```
qos trust {cos | dscp}
no qos trust
```

**Parameters**

- **cos** — Indicates that ingress packets are classified with packet CoS values. Untagged packets are classified with the default port CoS value.
- **dscp** — Indicates that ingress packets are classified with packet DSCP values.

**Default Setting**

CoS is the default trust mode.

**Command Mode**

Global Configuration mode

**Command Usage**

To disable QoS trust completely, use the **no qos** command. If **no qos trust** is used, trust VPT is set, and QoS trust is not disabled.

Packets entering a Quality of Service (QoS) domain are classified at the edge of the QoS domain. When packets are classified at the edge, the switch port within the QoS domain can be configured to one of the trusted states because there is no need to classify the packets at every device in the domain.

A switch port on an inter-QoS domain boundary can be configured to the DSCP trust state, and, if the DSCP values are different between the QoS domains, the DSCP to DSCP mutation map can be applied.

Use this command to specify whether the port is trusted and which fields of the packet to use to classify traffic.

When the system is configured as trust DSCP, traffic is mapped to a queue according to the DSCP-queue map.

The following table describes the VPT Default Mapping Table.

<table>
<thead>
<tr>
<th>VPT Value</th>
<th>Queue Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>3</td>
</tr>
</tbody>
</table>
Example

The following command configures the system to the DSCP trust state.

```
Console(config)# qos trust dscp
```
**qos cos**

The `qos cos` Interface Configuration (Ethernet, port-channel) mode command defines the default CoS value of a port. To return to the default configuration, use the `no` form of this command.

**Syntax**

```
qos cos default-cos
```

**Parameters**

- `default-cos` — Specifies the default CoS value of the port. (Range: 0-7)

**Default Setting**

Default CoS value of a port is 0.

**Command Mode**

Interface Configuration (Ethernet, port-channel) mode

**Command Usage**

If the port is trusted, the default CoS value of the port is used to assign a CoS value to all untagged packets entering the port.

**Example**

The following command configures port 1/e15 default CoS value to 3.

```
Console(config)# interface ethernet 1/e15
Console(config-if) qos cos 3
```
qos dscp-mutation

The **qos dscp-mutation** Global Configuration mode command applies the DSCP Mutation map to a system DSCP trusted port. To return to the trust state with no DSCP mutation, use the **no** form of this command.

**Syntax**

```
qos dscp-mutation
no qos dscp-mutation
```

**Parameters**

There are no parameters for this command.

**Default Setting**

This command has no default configuration.

**Command Mode**

Global Configuration mode.

**Command Usage**

The DSCP to DSCP mutation map is applied to a port at the boundary of a Quality of Service (QoS) administrative domain.

If two QoS domains have different DSCP definitions, use the DSCP to DSCP mutation map to match one set of DSCP values with the DSCP values of another domain.

Apply the DSCP to DSCP mutation map only to ingress and to DSCP-trusted ports. Applying this map to a port causes IP packets to be rewritten with newly mapped DSCP values at the ingress ports.

If the DSCP to DSCP mutation map is applied to an untrusted port, class of service (CoS) or IP-precedence trusted port, this command has no immediate effect until the port becomes DSCP-trusted.

**Example**

The following command applies the DSCP Mutation map to system DSCP trusted ports.

```
Console(config)# qos dscp-mutation
```
**qos map dscp-mutation**

The `qos map dscp-mutation` Global Configuration mode command modifies the DSCP to DSCP mutation map. To return to the default DSCP to DSCP mutation map, use the `no` form of this command.

**Syntax**

```
qos map dscp-mutation  in-dscp to out-dscp
no qos map dscp-mutation
```

**Parameters**

- `in-dscp` — Specifies up to 8 DSCP values separated by spaces. (Range: 0-63)
- `out-dscp` — Specifies up to 8 DSCP values separated by spaces. (Range: 0-63)

**Default Setting**

The default map is the Null map, which means that each incoming DSCP value is mapped to the same DSCP value.

**Command Mode**

Global Configuration mode.

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command changes DSCP values 1, 2, 4, 5 and 6 to DSCP mutation map value 63.

```
Console(config)# qos map dscp-mutation 1 2 4 5 6 to 63
```
radius-server host

The `radius-server host` Global Configuration mode command specifies a RADIUS server host. To delete the specified RADIUS host, use the `no` form of this command.

**Syntax**

```
radius-server host {ip-address | hostname} [auth-port auth-port-number] [timeout timeout] [retransmit retries] [deadtime deadtime] [key key-string] [source source] [priority priority]
no radius-server host {ip-address | hostname}
```

**Parameters**

- `ip-address` — IP address of the RADIUS server host.
- `hostname` — Hostname of the RADIUS server host. (Range: 1-158 characters)
- `auth-port-number` — Port number for authentication requests. The host is not used for authentication if the port number is set to 0. (Range: 0-65535)
- `timeout` — Specifies the timeout value in seconds. (Range: 1-30)
- `retries` — Specifies the retransmit value. (Range: 1-10)
- `deadtime` — Length of time in minutes during which a RADIUS server is skipped over by transaction requests. (Range: 0-2000)
- `key-string` — Specifies the authentication and encryption key for all RADIUS communications between the device and the RADIUS server. This key must match the RADIUS daemon key used on the RADIUS daemon. To specify an empty string, enter “”. (Range: 0-128 characters)
- `source` — Specifies the source IP address to use for communication. 0.0.0.0 is interpreted as request to use the IP address of the outgoing IP interface.
- `priority` — Determines the order in which servers are used, where 0 has the highest priority. (Range: 0-65535)
- `usage` — Specifies the usage type of the server. Can be one of the following values: login, dot.1x or all. If unspecified, defaults to all.

**Default Setting**

No RADIUS server host is specified.

The port number for authentication requests is 1812.

The usage type is all.

**Command Mode**

Global Configuration mode
**Command Usage**

To specify multiple hosts, multiple `radius-server host` commands can be used.

If no host-specific timeout, retries, deadtime or key-string values are specified, global values apply to each RADIUS server host.

The address type of the source parameter must be the same as the `ip-address` parameter.

**Example**

The following command specifies a RADIUS server host with IP address 192.168.10.1, authentication request port number 20 and a 20-second timeout period.

```
Console(config)# radius-server host 192.168.10.1 auth-port 20 timeout 20
```
radius-server key

The radius-server key Global Configuration mode command sets the authentication and encryption key for all RADIUS communications between the device and the RADIUS daemon. To return to the default configuration, use the no form of this command.

Syntax

radius-server key [key-string]
no radius-server key

Parameters

- key-string — Specifies the authentication and encryption key for all RADIUS communications between the device and the RADIUS server. This key must match the RADIUS daemon key used on the RADIUS daemon. (Range: 0-128 characters)

Default Setting

The key-string is an empty string.

Command Mode

Global Configuration mode

Command Usage

There are no user guidelines for this command.

Example

The following command defines the authentication and encryption key for all RADIUS communications between the device and the RADIUS daemon.

```
Console(config)# radius-server key hp-server
```
radius-server retransmit

The radius-server retransmit Global Configuration mode command specifies the number of times the software searches the list of RADIUS server hosts. To reset the default configuration, use the no form of this command.

Syntax

radius-server retransmit retries
no radius-server retransmit

Parameters

- retries — Specifies the retransmit value. (Range: 1-10)

Default Setting

The software searches the list of RADIUS server hosts 3 times.

Command Mode

Global Configuration mode

Command Usage

There are no user guidelines for this command.

Example

The following command configures the number of times the software searches the list of RADIUS server hosts to 5 times.

Console(config)# radius-server retransmit 5
**radius-server source-ip**

The *radius-server source-ip* Global Configuration mode command specifies the source IP address used for communication with RADIUS servers. To return to the default configuration, use the *no* form of this command.

**Syntax**

- `radius-server source-ip source`
- `no radius-source-ip source`

**Parameters**

- `source` — Specifies a valid source IP address.

**Default Setting**

The source IP address is the IP address of the outgoing IP interface.

**Command Mode**

Global Configuration mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command configures the source IP address used for communication with RADIUS servers to 10.1.1.1.

```
Console(config)# radius-server source-ip 10.1.1.1
```
radius-server timeout

The radius-server timeout Global Configuration mode command sets the interval during which the device waits for a server host to reply. To return to the default configuration, use the no form of this command.

Syntax

radius-server timeout timeout
no radius-server timeout

Parameters

■ timeout — Specifies the timeout value in seconds. (Range: 1-30)

Default Setting

The timeout value is 3 seconds.

Command Mode

Global Configuration mode

Command Usage

There are no user guidelines for this command.

Example

The following command configures the timeout interval to 5 seconds.

```
Console(config)# radius-server timeout 5
```
radius-server deadtime

The `radius-server deadtime` Global Configuration mode command improves RADIUS response time when servers are unavailable. The command is used to cause the unavailable servers to be skipped. To return to the default configuration, use the `no` form of this command.

**Syntax**

`radius-server deadtime deadtime`

`no radius-server deadtime`

**Parameters**

- `deadtime` — Length of time in minutes during which a RADIUS server is skipped over by transaction requests. (Range: 0-2000)

**Default Setting**

The deadtime setting is 0.

**Command Mode**

Global Configuration mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command sets the deadtime to 10 minutes.

```
Console(config)# radius-server deadtime 10
```
**show radius-servers**

The `show radius-servers` Privileged EXEC mode command displays the RADIUS server settings.

**Syntax**

`show radius-servers`

**Parameters**

There are no parameters for this command.

**Default Setting**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command displays RADIUS server settings.

```console
Console# show radius-servers

<table>
<thead>
<tr>
<th>IP address</th>
<th>Authin CLI</th>
<th>TimeOut</th>
<th>Retran in CLI</th>
<th>DeadTime</th>
<th>Source in CLI</th>
<th>Prio in CLI</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.1.1</td>
<td>1645</td>
<td>Global</td>
<td>Global</td>
<td>Global</td>
<td>-</td>
<td>1</td>
<td>All</td>
</tr>
<tr>
<td>172.16.1.2</td>
<td>1645</td>
<td>11</td>
<td>8</td>
<td>Global</td>
<td>Global</td>
<td>2</td>
<td>All</td>
</tr>
</tbody>
</table>

Global values

-------------
TimeOut: 3
Retransmit: 3
Deadtime: 0
Source IP: 172.16.8.1
```
show rmon statistics

The **show rmon statistics** User EXEC mode command displays RMON Ethernet statistics.

**Syntax**

*show rmon statistics { ethernet interface number | port-channel port-channel-number}*

**Parameters**

- **interface number** — Valid Ethernet port.
- **port-channel-number** — Valid port-channel number.

**Default Setting**

This command has no default configuration.

**Command Mode**

User EXEC mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command displays RMON Ethernet statistics for Ethernet port 1/e1.

```
Console> show rmon statistics ethernet 1/e1

Port: 1/e1
Octets: 878128  Packets: 978
Broadcast: 7    Multicast: 1
CRC Align Errors: 0  Collisions: 0
Undersize Pkts: 0    Oversize Pkts: 0
Fragments: 0  Jabbers: 0
64 Octets: 98  65 to 127 Octets: 0
128 to 255 Octets: 0  256 to 511 Octets: 0
512 to 1023 Octets: 491  1024 to 1518 Octets: 389
```
The following table describes significant fields shown in the example:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Octets</td>
<td>The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>Packets</td>
<td>The total number of packets (including bad packets, broadcast packets, and multicast packets) received.</td>
</tr>
<tr>
<td>Broadcast</td>
<td>The total number of good packets received and directed to the broadcast address. This does not include multicast packets.</td>
</tr>
<tr>
<td>Multicast</td>
<td>The total number of good packets received and directed to a multicast address. This number does not include packets directed to the broadcast address.</td>
</tr>
<tr>
<td>CRC Align Errors</td>
<td>The total number of packets received with a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but with 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).</td>
</tr>
<tr>
<td>Collisions</td>
<td>The best estimate of the total number of collisions on this Ethernet segment.</td>
</tr>
<tr>
<td>Undersize Pkts</td>
<td>The total number of packets received less than 64 octets long (excluding framing bits, but including FCS octets) and otherwise well formed.</td>
</tr>
<tr>
<td>Oversize Pkts</td>
<td>The total number of packets received longer than 1518 octets (excluding framing bits, but including FCS octets) and otherwise well formed.</td>
</tr>
<tr>
<td>Fragments</td>
<td>The total number of packets received less than 64 octets in length (excluding framing bits but including FCS octets) and 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).</td>
</tr>
<tr>
<td>Jabbers</td>
<td>The total number of packets received longer than 1518 octets (excluding framing bits, but including FCS octets), and 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).</td>
</tr>
<tr>
<td>64 Octets</td>
<td>The total number of packets (including bad packets) received that are 64 octets in length (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>65 to 127 Octets</td>
<td>The total number of packets (including bad packets) received that are between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>128 to 255 Octets</td>
<td>The total number of packets (including bad packets) received that are between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>256 to 511 Octets</td>
<td>The total number of packets (including bad packets) received that are between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>512 to 1023 Octets</td>
<td>The total number of packets (including bad packets) received that are between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>1024 to 1518 Octets</td>
<td>The total number of packets (including bad packets) received that are between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).</td>
</tr>
</tbody>
</table>
rmon collection history

The **rmon collection history** Interface Configuration (Ethernet, port-channel) mode command enables a Remote Monitoring (RMON) MIB history statistics group on an interface. To remove a specified RMON history statistics group, use the **no** form of this command.

**Syntax**

```
rmon collection history index [owner ownername] [buckets bucket-number] [interval seconds]
no rmon collection history index
```

**Parameters**

- **index** — Specifies the statistics group index. (Range: 1-65535)
- **ownername** — Specifies the RMON statistics group owner name.
- **bucket-number** — Number of buckets specified for the RMON collection history group of statistics. If unspecified, defaults to 50. (Range:1-65535)
- **seconds** — Number of seconds in each polling cycle. (Range: 1-3600)

**Default Setting**

RMON statistics group owner name is an empty string.
Number of buckets specified for the RMON collection history statistics group is 50.
Number of seconds in each polling cycle is 1800.

**Command Mode**

Interface Configuration (Ethernet, port-channel) mode

**Command Usage**

Cannot be configured for a range of interfaces (range context).

**Example**

The following command enables a Remote Monitoring (RMON) MIB history statistics group on Ethernet port 1/e1 with index number 1 and a polling interval period of 2400 seconds.

```
Console(config)# interface ethernet 1/e1
Console(config-if)# rmon collection history 1 interval 2400
```
**show rmon collection history**

The **show rmon collection history** User EXEC mode command displays the requested RMON history group statistics.

**Syntax**

```
show rmon collection history [ethernet interface | port-channel port-channel-number]
```

**Parameters**

- **interface** — Valid Ethernet port. (Full syntax: `port`)
- **port-channel-number** — Valid port-channel number.

**Default Setting**

This command has no default configuration.

**Command Mode**

User EXEC mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command displays all RMON history group statistics.

```
Console> show rmon collection history
```

<table>
<thead>
<tr>
<th>Index</th>
<th>Interface</th>
<th>Interval</th>
<th>Requested Samples</th>
<th>Granted Samples</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1/e1</td>
<td>30</td>
<td>50</td>
<td>50</td>
<td>CLI</td>
</tr>
<tr>
<td>2</td>
<td>1/e1</td>
<td>1800</td>
<td>50</td>
<td>50</td>
<td>Manager</td>
</tr>
</tbody>
</table>

The following table describes significant fields shown in the example:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>An index that uniquely identifies the entry.</td>
</tr>
<tr>
<td>Interface</td>
<td>The sampled Ethernet interface.</td>
</tr>
<tr>
<td>Interval</td>
<td>The interval in seconds between samples.</td>
</tr>
<tr>
<td>Requested Samples</td>
<td>The requested number of samples to be saved.</td>
</tr>
<tr>
<td>Granted Samples</td>
<td>The granted number of samples to be saved.</td>
</tr>
<tr>
<td>Owner</td>
<td>The entity that configured this entry.</td>
</tr>
</tbody>
</table>
**show rmon history**

The **show rmon history** User EXEC mode command displays RMON Ethernet history statistics.

**Syntax**

```
show rmon history index {throughput | errors | other} [period seconds]
```

**Parameters**

- `index` — Specifies the requested set of samples. (Range: 1-65535)
- `throughput` — Indicates throughput counters.
- `errors` — Indicates error counters.
- `other` — Indicates drop and collision counters.
- `seconds` — Specifies the period of time in seconds. (Range: 1-4294967295)

**Default Setting**

This command has no default configuration.

**Command Mode**

User EXEC mode

**Command Usage**

There are no user guidelines for this command.

**Examples**

The following command displays RMON Ethernet history statistics for index 1.

```
Console> show rmon history 1 throughput

Sample Set: 1 Owner: CLI
Interface: 1/e1 Interval: 1800
Requested samples: 50 Granted samples: 50

Maximum table size: 500

<table>
<thead>
<tr>
<th>Time</th>
<th>Octets</th>
<th>Packets</th>
<th>Broadcast</th>
<th>Multicast</th>
<th>Util</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jan 18 2005 21:57:00</td>
<td>303595962</td>
<td>357568</td>
<td>3289</td>
<td>7287</td>
<td>19%</td>
</tr>
<tr>
<td>Jan 18 2005 21:57:30</td>
<td>287696304</td>
<td>275686</td>
<td>2789</td>
<td>5878</td>
<td>20%</td>
</tr>
</tbody>
</table>

Console> show rmon history 1 errors

Sample Set: 1 Owner: Me
Interface: 1/e1 Interval: 1800
Requested samples: 50 Granted samples: 50

<table>
<thead>
<tr>
<th>Time</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```
RMON Commands

The following table describes significant fields shown in the example:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>Date and Time the entry is recorded.</td>
</tr>
<tr>
<td>Octets</td>
<td>The total number of octets of data (including those in bad packets) received on the network.</td>
</tr>
<tr>
<td>Packets</td>
<td>The number of packets (including bad packets) received during this sampling interval.</td>
</tr>
<tr>
<td>Broadcast</td>
<td>The number of good packets received during this sampling interval that were directed to the broadcast address.</td>
</tr>
<tr>
<td>Multicast</td>
<td>The number of good packets received during this sampling interval that were directed to a multicast address. This number does not include packets addressed to the broadcast address.</td>
</tr>
<tr>
<td>Util</td>
<td>The best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.</td>
</tr>
<tr>
<td>CRC Align</td>
<td>The number of packets received during this sampling interval that had a length (excluding framing bits but including FCS octets) between 64 and 1518 octets, inclusive, but 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).</td>
</tr>
<tr>
<td>Undersize</td>
<td>The number of packets received during this sampling interval that were less than 64 octets long (excluding framing bits but including FCS octets) and were otherwise well formed.</td>
</tr>
<tr>
<td>Oversize</td>
<td>The number of packets received during this sampling interval that were longer than 1518 octets (excluding framing bits but including FCS octets) but were otherwise well formed.</td>
</tr>
</tbody>
</table>
### RMON Commands

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fragments</td>
<td>The total number of packets received during this sampling interval that were less than 64 octets in length (excluding framing bits but including FCS octets) 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 (AlignmentError). It is normal for etherHistoryFragments to increment because it counts both runts (which are normal occurrences due to collisions) and noise hits.</td>
</tr>
<tr>
<td>Jabbers</td>
<td>The number of packets received during this sampling interval 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).</td>
</tr>
<tr>
<td>Dropped</td>
<td>The total number of events in which packets were dropped by the probe due to lack of resources during this sampling interval. This number is not necessarily the number of packets dropped, it is just the number of times this condition has been detected.</td>
</tr>
<tr>
<td>Collisions</td>
<td>The best estimate of the total number of collisions on this Ethernet segment during this sampling interval.</td>
</tr>
</tbody>
</table>
**rmon alarm**

The **rmon alarm** Global Configuration mode command configures alarm conditions. To remove an alarm, use the **no** form of this command.

**Syntax**

```
rmon alarm index variable interval rthreshold fthreshold revent fevent [type type] [startup direction] [owner name]
```

```
no rmon alarm index
```

**Parameters**

- **index** — Specifies the alarm index. (Range: 1-65535)
- **variable** — Specifies the object identifier of the variable to be sampled.
- **interval** — Specifies the interval in seconds during which the data is sampled and compared with rising and falling thresholds. (Range: 1-4294967295)
- **rthreshold** — Specifies the rising threshold. (Range: 0-4294967295)
- **fthreshold** — Specifies the falling threshold. (Range: 0-4294967295)
- **revent** — Specifies the event index used when a rising threshold is crossed. (Range: 1-65535)
- **fevent** — Specifies the event index used when a falling threshold is crossed. (Range: 1-65535)
- **type** — Specifies the method used for sampling the selected variable and calculating the value to be compared against the thresholds. Possible values are **absolute** and **delta**.

- If the method is **absolute**, the value of the selected variable is compared directly with the thresholds at the end of the sampling interval. If the method is **delta**, the selected variable value of the last sample is subtracted from the current value, and the difference is compared with the thresholds.
- **direction** — Specifies the alarm that may be sent when this entry is first set to valid. Possible values are **rising**, **rising-falling** and **falling**.

If the first sample (after this entry becomes valid) is greater than or equal to **rthreshold** and **direction** is equal to **rising** or **rising-falling**, a single rising alarm is generated. If the first sample (after this entry becomes valid) is less than or equal to **fthreshold** and **direction** is equal to **falling** or **rising-falling**, a single falling alarm is generated.

- **name** — Specifies the name of the person who configured this alarm. If unspecified, the name is an empty string.

**Default Setting**

The type is **absolute**.

The startup direction is **rising-falling**.

**Command Mode**

Global Configuration mode

**Command Usage**

There are no user guidelines for this command.
Example

The following command configures the following alarm conditions:

- Alarm index — 1000
- Variable identifier — HP
- Sample interval — 360000 seconds
- Rising threshold — 1000000
- Falling threshold — 1000000
- Rising threshold event index — 10
- Falling threshold event index — 20

```
Console(config)# rmon alarm 1000 HP 360000 1000000 1000000 10 20
```
**show rmon alarm-table**

The `show rmon alarm-table` User EXEC mode command displays the alarms table.

**Syntax**

`show rmon alarm-table`

**Parameters**

There are no parameters for this command.

**Default Setting**

This command has no default configuration.

**Command Mode**

User EXEC mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command displays the alarms table.

```
Console> show rmon alarm-table

<table>
<thead>
<tr>
<th>Index</th>
<th>OID</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1.3.6.1.2.1.2.2.1.10.1</td>
<td>CLI</td>
</tr>
<tr>
<td>2</td>
<td>1.3.6.1.2.1.2.2.1.10.1</td>
<td>Manager</td>
</tr>
<tr>
<td>3</td>
<td>1.3.6.1.2.1.2.2.1.10.9</td>
<td>CLI</td>
</tr>
</tbody>
</table>
```

The following table describes significant fields shown in the example:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>An index that uniquely identifies the entry.</td>
</tr>
<tr>
<td>OID</td>
<td>Monitored variable OID.</td>
</tr>
<tr>
<td>Owner</td>
<td>The entity that configured this entry.</td>
</tr>
</tbody>
</table>
show rmon alarm

The show rmon alarm User EXEC mode command displays alarm configuration.

Syntax

show rmon alarm number

Parameters

- number — Specifies the alarm index. (Range: 1-65535)

Default Setting

This command has no default configuration.

Command Mode

User EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following command displays RMON 1 alarms.

```
   Console> show rmon alarm 1

   Alarm 1
   ------
   OID: 1.3.6.1.2.1.2.2.1.10.1
   Last sample Value: 878128
   Interval: 30
   Sample Type: delta
   Startup Alarm: rising
   Rising Threshold: 8700000
   Falling Threshold: 78
   Rising Event: 1
   Falling Event: 1
   Owner: CLI
```

The following table describes the significant fields shown in the example:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarm</td>
<td>Alarm index.</td>
</tr>
<tr>
<td>OID</td>
<td>Monitored variable OID.</td>
</tr>
</tbody>
</table>
## RMON Commands

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Sample Value</td>
<td>The statistic value during the last sampling period. For example, if the sample type is <code>delta</code>, this value is the difference between the samples at the beginning and end of the period. If the sample type is <code>absolute</code>, this value is the sampled value at the end of the period.</td>
</tr>
<tr>
<td>Interval</td>
<td>The interval in seconds over which the data is sampled and compared with the rising and falling thresholds.</td>
</tr>
<tr>
<td>Sample Type</td>
<td>The method of sampling the variable and calculating the value compared against the thresholds. If the value is <code>absolute</code>, the value of the variable is compared directly with the thresholds at the end of the sampling interval. If the value is <code>delta</code>, the value of the variable at the last sample is subtracted from the current value, and the difference compared with the thresholds.</td>
</tr>
<tr>
<td>Startup Alarm</td>
<td>The alarm that may be sent when this entry is first set. If the first sample is greater than or equal to the rising threshold, and startup alarm is equal to rising or rising and falling, then a single rising alarm is generated. If the first sample is less than or equal to the falling threshold, and startup alarm is equal falling or rising and falling, then a single falling alarm is generated.</td>
</tr>
<tr>
<td>Rising Threshold</td>
<td>A sampled statistic threshold. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval is less than this threshold, a single event is generated.</td>
</tr>
<tr>
<td>Falling Threshold</td>
<td>A sampled statistic threshold. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval is greater than this threshold, a single event is generated.</td>
</tr>
<tr>
<td>Rising Event</td>
<td>The event index used when a rising threshold is crossed.</td>
</tr>
<tr>
<td>Falling Event</td>
<td>The event index used when a falling threshold is crossed.</td>
</tr>
<tr>
<td>Owner</td>
<td>The entity that configured this entry.</td>
</tr>
</tbody>
</table>
**rmon event**

The **rmon event** Global Configuration mode command configures an event. To remove an event, use the **no** form of this command.

**Syntax**

```
rmon event index type [community text] [description text] [owner name]
no rmon event index
```

**Parameters**

- **index** — Specifies the event index. (Range: 1-65535)
- **type** — Specifies the type of notification generated by the device about this event. Possible values: **none, log, trap, log-trap**.
- **community text** — If the specified notification type is **trap**, an SNMP trap is sent to the SNMP community specified by this octet string. (Range: 0-127 characters)
- **description text** — Specifies a comment describing this event. (Range: 0-127 characters)
- **name** — Specifies the name of the person who configured this event. If unspecified, the name is an empty string.

**Default Setting**

This command has no default configuration.

**Command Mode**

Global Configuration mode

**Command Usage**

If **log** is specified as the notification type, an entry is made in the log table for each event. If **trap** is specified, an SNMP trap is sent to one or more management stations.

**Example**

The following command configures an event identified as index 10 and for which the device generates a notification in the log table.

```
Console(config)# rmon event 10 log
```
show rmon events

The `show rmon events` User EXEC mode command displays the RMON event table.

**Syntax**

`show rmon events`

**Parameters**

There are no parameters for this command.

**Default Setting**

This command has no default configuration.

**Command Mode**

User EXEC mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command displays the RMON events table.

```
Console> show rmon events

<table>
<thead>
<tr>
<th>Index</th>
<th>Description</th>
<th>Type</th>
<th>Community</th>
<th>Owner</th>
<th>Last Time Sent</th>
</tr>
</thead>
<tbody>
<tr>
<td>---</td>
<td>-----------</td>
<td>------</td>
<td>-----------</td>
<td>-------</td>
<td>-------------------</td>
</tr>
<tr>
<td>1</td>
<td>Errors</td>
<td>Log</td>
<td>CLI</td>
<td>Jan 18 2005 23:58:17</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>High Broadcast</td>
<td>Log-Trap</td>
<td>device Manager</td>
<td>Jan 18 2005 23:59:48</td>
<td></td>
</tr>
</tbody>
</table>
```

The following table describes significant fields shown in the example:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>An index that uniquely identifies the event.</td>
</tr>
<tr>
<td>Description</td>
<td>A comment describing this event.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of notification that the device generates about this event. Can have the following values: <code>none</code>, <code>log</code>, <code>trap</code>, <code>log-trap</code>. In the case of log, an entry is made in the log table for each event. In the case of trap, an SNMP trap is sent to one or more management stations.</td>
</tr>
<tr>
<td>Community</td>
<td>If an SNMP trap is to be sent, it is sent to the SNMP community specified by this octet string.</td>
</tr>
<tr>
<td>Owner</td>
<td>The entity that configured this event.</td>
</tr>
<tr>
<td>Last time sent</td>
<td>The time this entry last generated an event. If this entry has not generated any events, this value is zero.</td>
</tr>
</tbody>
</table>
show rmon log

The `show rmon log` User EXEC mode command displays the RMON log table.

**Syntax**

`show rmon log [event]`

**Parameters**

- `event` — Specifies the event index. (Range: 0 - 65535)

**Default Setting**

This command has no default configuration.

**Command Mode**

User EXEC mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command displays the RMON log table.

```
Console> show rmon log

Maximum table size: 500
Event  Description       Time
------- ------------------ --------
1       Errors          Jan 18 2005 23:48:19
1       Errors          Jan 18 2005 23:58:17

Console> show rmon log 1

Maximum table size: 500 (800 after reset)
Event  Description       Time
------- ------------------ --------
1       Errors          Jan 18 2005 23:48:19
1       Errors          Jan 18 2005 23:58:17
```

The following table describes the significant fields shown in the display:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event</td>
<td>An index that uniquely identifies the event.</td>
</tr>
<tr>
<td>Description</td>
<td>A comment describing this event.</td>
</tr>
<tr>
<td>Time</td>
<td>The time this entry was created.</td>
</tr>
</tbody>
</table>
rmon table-size

The **rmon table-size** Global Configuration mode command configures the maximum size of RMON tables. To return to the default configuration, use the **no** form of this command.

**Syntax**

```plaintext
rmon table-size {history entries | log entries}
normon table-size {history | log}
```

**Parameters**

- **history entries** — Maximum number of history table entries. (Range: 20-270)
- **log entries** — Maximum number of log table entries. (Range: 20-100)

**Default Setting**

History table size is 270.
Log table size is 200.

**Command Mode**

Global Configuration mode

**Command Usage**

The configured table size takes effect after the device is rebooted.

**Example**

The following command configures the maximum RMON history table sizes to 100 entries.

```plaintext
Console(config)# rmon table-size history 100
```
snmp-server community

The `snmp-server community` Global Configuration mode command configures the community access string to permit access to the SNMP protocol. To remove the specified community string, use the **no** form of this command.

**Syntax**

```plaintext
snmp-server community community [ro | rw | su] [ip-address] [view view-name]

snmp-server community-group community group-name [ip-address]

no snmp-server community community [ip-address]
```

**Parameters**

- **community** — Community string that acts like a password and permits access to the SNMP protocol. (Range: 1-20 characters)
- **ro** — Indicates read-only access (default).
- **rw** — Indicates read-write access.
- **su** — Indicates SNMP administrator access.
- **ip-address** — Specifies the IP address of the management station.
- **group-name** — Specifies the name of a previously defined group. A group defines the objects available to the community. (Range: 1-30 characters)
- **view-name** — Specifies the name of a previously defined view. The view defines the objects available to the community. (Range: 1-30 characters)

**Default Setting**

The community PUBLIC is set with read-only access. No write communities are defined by default.

**Command Mode**

Global Configuration mode

**Command Usage**

The **view-name** parameter cannot be specified for **su**, which has access to the whole MIB.

The **view-name** parameter can be used to restrict the access rights of a community string. When it is specified:

An internal security name is generated.

The internal security name for SNMPv1 and SNMPv2 security models is mapped to an internal group name.
The internal group name for SNMPv1 and SNMPv2 security models is mapped to a view-name (read-view and notify-view always, and for rw for write-view also).

The **group-name** parameter can also be used to restrict the access rights of a community string. When it is specified:

An internal security name is generated.

The internal security name for SNMPv1 and SNMPv2 security models is mapped to the group name.

**Example**

The following command defines community access string **public** to permit administrative access to SNMP protocol at an administrative station with IP address 192.168.1.20.

```
Console(config)# snmp-server community public su 192.168.1.20
```
snmp-server view

The `snmp-server view` Global Configuration mode command creates or updates a Simple Network Management Protocol (SNMP) server view entry. To remove a specified SNMP server view entry, use the `no` form of this command.

**Syntax**

```
snmp-server view view-name oid-tree { included | excluded }
no snmp-server view view-name [oid-tree]
```

**Parameters**

- `view-name` — Specifies the label for the view record that is being created or updated. The name is used to reference the record. (Range: 1-30 characters)
- `oid-tree` — Specifies the object identifier of the ASN.1 subtree to be included or excluded from the view. To identify the subtree, specify a text string consisting of numbers, such as 1.3.6.2.4, or a word, such as system. Replace a single sub-identifier with the asterisk (*) wildcard to specify a subtree family; for example 1.3.*.4.
- `included` — Indicates that the view type is included.
- `excluded` — Indicates that the view type is excluded.

**Default Setting**

No view entry exists.

**Command Mode**

Global Configuration mode

**Command Usage**

This command can be entered multiple times for the same view record. The number of views is limited to 64.

No check is made to determine that a MIB node corresponds to the “starting portion” of the OID until the first wildcard.

**Example**

The following command creates a view that includes all objects in the MIB-II system group except for sysServices (System 7) and all objects for interface 1 in the MIB-II interface group.

```
Console(config)# snmp-server view user-view system included
Console(config)# snmp-server view user-view system.7 excluded
Console(config)# snmp-server view user-view ifEntry.*.1 included
```
**snmp-server group**

The `snmp-server group` Global Configuration mode command configures a new Simple Management Protocol (SNMP) group or a table that maps SNMP users to SNMP views. To remove a specified SNMP group, use the `no` form of this command.

**Syntax**

```
snmp-server group groupname {v1 | v2 | v3 {noauth | auth | priv} [notify notifyview]} [read readview] [write writeview]
no snmp-server group groupname {v1 | v2 | v3 [noauth | auth | priv]}
```

**Parameters**

- `groupname`—Specifies the name of the group.
- `v1`—Indicates the SNMP Version 1 security model.
- `v2`—Indicates the SNMP Version 2 security model.
- `v3`—Indicates the SNMP Version 3 security model.
- `noauth`—Indicates no authentication of a packet. Applicable only to the SNMP Version 3 security model.
- `auth`—Indicates authentication of a packet without encrypting it. Applicable only to the SNMP Version 3 security model.
- `priv`—Indicates authentication of a packet with encryption. Applicable only to the SNMP Version 3 security model.
- `readview`—Specifies a string that is the name of the view that enables only viewing the contents of the agent. If unspecified, all objects except for the community-table and SNMPv3 user and access tables are available.
- `writeview`—Specifies a string that is the name of the view that enables entering data and configuring the contents of the agent. If unspecified, nothing is defined for the write view.
- `notifyview`—Specifies a string that is the name of the view that enables specifying an inform or a trap. If unspecified, nothing is defined for the notify view. Applicable only to the SNMP Version 3 security model.

**Default Setting**

No group entry exists.

**Command Mode**

Global Configuration mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command attaches a group called user-group to SNMPv3 and assigns to the group the privacy security level and read access rights to a view called user-view.

```
Console(config)# snmp-server group user-group v3 priv read user-view
```
snmp-server user

The `snmp-server user` Global Configuration mode command configures a new SNMP Version 3 user. To remove a user, use the `no` form of this command.

**Syntax**

```
snmp-server user username groupname [remote engineid-string] [auth-md5 password | auth-sha password | auth-md5-key md5-des-keys | auth-sha-key sha-des-keys]
```

```
o snmp-server user username [remote engineid-string]
```

**Parameters**

- `username` — Specifies the name of the user on the host that connects to the agent. (Range: 1-30 characters)
- `groupname` — Specifies the name of the group to which the user belongs. (Range: 1-30 characters)
- `engineid-string` — Specifies the engine ID of the remote SNMP entity to which the user belongs. The engine ID is a concatenated hexadecimal string. Each byte in the hexadecimal character string is two hexadecimal digits. Each byte can be separated by a period or colon. (Range: `engineID` must contain from 9 through 64 hexadecimal digits)
- `auth-md5 password` — Indicates the HMAC-MD5-96 authentication level. The user should enter a password for authentication and generation of a DES key for privacy. (Range: 1-32 characters)
- `auth-sha password` — Indicates the HMAC-SHA-96 authentication level. The user should enter a password for authentication and generation of a DES key for privacy. (Range: 1-32 characters)
- `auth-md5-key md5-des-keys` — Indicates the HMAC-MD5-96 authentication level. The user should enter a concatenated hexadecimal string of the MD5 key (MSB) and the privacy key (LSB). If authentication is only required, 16 bytes should be entered; if authentication and privacy are required, 32 bytes should be entered. Each byte in the hexadecimal character string is two hexadecimal digits. Each byte can be separated by a period or colon. (16 or 32 bytes)
- `auth-sha-key sha-des-keys` — Indicates the HMAC-SHA-96 authentication level. The user should enter a concatenated hexadecimal string of the SHA key (MSB) and the privacy key (LSB). If authentication is only required, 20 bytes should be entered; if authentication and privacy are required, 36 bytes should be entered. Each byte in the hexadecimal character string is two hexadecimal digits. Each byte can be separated by a period or colon. (20 or 36 bytes)

**Default Setting**

No group entry exists.

**Command Mode**

Global Configuration mode

**Command Usage**

If auth-md5 or auth-sha is specified, both authentication and privacy are enabled for the user.
When a **show running-config** Privileged EXEC mode command is entered, a line for this user will not be displayed. To see if this user has been added to the configuration, type the **show snmp users** Privileged EXEC mode command.

An SNMP EngineID has to be defined to add SNMP users to the device. Changing or removing the SNMP EngineID value deletes SNMPv3 users from the device’s database.

The remote engineid designates the remote management station and should be defined to enable the device to receive informs.

**Example**

The following command configures an SNMPv3 user **John** in group **user-group**.

```
Console(config)# snmp-server user John user-group
```
snmp-server engineid local

The `snmp-server engineid local` Global Configuration mode command specifies the Simple Network Management Protocol (SNMP) engine ID on the local device. To remove the configured engine ID, use the `no` form of this command.

**Syntax**

```
snmp-server engineid local {engineid-string | default}
no snmp-server engineid local
```

**Parameters**

- `engineid-string` — Specifies a character string that identifies the engine ID.
  (Range: engine ID must contain from 9 through 64 hexadecimal digits)
- `default` — The engine ID is created automatically based on the device MAC address.

**Default Setting**

The engine ID is not configured.

If SNMPv3 is enabled using this command, and the default is specified, the default engine ID is defined per standard as:

- First 4 octets — first bit = 1, the rest is IANA Enterprise number = 674.
- Fifth octet — set to 3 to indicate the MAC address that follows.
- Last 6 octets — MAC address of the device.

**Command Mode**

Global Configuration mode

**Command Usage**

To use SNMPv3, you have to specify an engine ID for the device. You can specify your own ID or use a default string that is generated using the MAC address of the device.

If the SNMPv3 engine ID is deleted or the configuration file is erased, SNMPv3 cannot be used. By default, SNMPv1/v2 are enabled on the device. SNMPv3 is enabled only by defining the Local Engine ID.

If you want to specify your own ID, you do not have to specify the entire 32-character engine ID if it contains trailing zeros. Specify only the portion of the engine ID up to the point where just zeros remain in the value. For example, to configure an engine ID of 123400000000000000000000, you can specify `snmp-server engineID local 1234`.

Since the engine ID should be unique within an administrative domain, the following is recommended:

For a standalone device, use the default keyword to configure the engine ID.

Changing the value of the engine ID has the following important side-effect. A user's password (entered on the command line) is converted to an MD5 or SHA security digest. This digest is based on both the password and the local engine ID. The user's command line password is then destroyed, as required by RFC 2274. As a result, the security digests of SNMPv3 users become invalid if the local value of the engine ID change, and the users will have to be reconfigured.

You cannot specify an engine ID that consists of all 0x0, all 0xF or 0x00000001.
The `show running-config` Privileged EXEC mode command does not display the SNMP engine ID configuration. To see the SNMP engine ID configuration, enter the `show snmp engineid` Global Configuration mode command.

**Example**

The following command enables SNMPv3 on the device and sets the local engine ID of the device to the default value.

```
Console(config)# snmp-server engineid local default
```
**snmp-server enable traps**

The `snmp-server enable traps` Global Configuration mode command enables the device to send SNMP traps. To disable SNMP traps, use the `no` form of the command.

**Syntax**

`snmp-server enable traps`

`no snmp-server enable traps`

**Parameters**

There are no parameters for this command.

**Default Setting**

SNMP traps are enabled.

**Command Mode**

Global Configuration mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command enables SNMP traps.

```
Console(config)# snmp-server enable traps
```
**snmp-server filter**

The `snmp-server filter` Global Configuration mode command creates or updates a Simple Network Management Protocol (SNMP) server filter entry. To remove the specified SNMP server filter entry, use the `no` form of this command.

**Syntax**

```
snmp-server filter filter-name oid-tree { included | excluded }
no snmp-server filter filter-name [oid-tree]
```

**Parameters**

- **filter-name** — Specifies the label for the filter record that is being updated or created. The name is used to reference the record. (Range: 1-30 characters)
- **oid-tree** — Specifies the object identifier of the ASN.1 subtree to be included or excluded from the view. To identify the subtree, specify a text string consisting of numbers, such as 1.3.6.2.4, or a word, such as system. Replace a single sub-identifier with the asterisk (*) wildcard to specify a subtree family; for example, 1.3.*.4.
- **included** — Indicates that the filter type is included.
- **excluded** — Indicates that the filter type is excluded.

**Default Setting**

No filter entry exists.

**Command Mode**

Global Configuration mode

**Command Usage**

This command can be entered multiple times for the same filter record. Later lines take precedence when an object identifier is included in two or more lines.

**Example**

The following command creates a filter that includes all objects in the MIB-II system group except for `sysServices` (System 7) and all objects for interface 1 in the MIB-II interfaces group.

```
Console(config)# snmp-server filter filter-name system included
Console(config)# snmp-server filter filter-name system.7 excluded
Console(config)# snmp-server filter filter-name ifEntry.*.1 included
```
snmp-server host

The **snmp-server host** Global Configuration mode command specifies the recipient of Simple Network Management Protocol Version 1 or Version 2 notifications. To remove the specified host, use the **no** form of this command.

**Syntax**

```
snmp-server host {ip-address | hostname} community-string [traps | informs] [1 | 2] [udp-port port] [filter filtername] [timeout seconds] [retries retries]
```

```
no snmp-server host {ip-address | hostname} [traps | informs]
```

**Parameters**

- **ip-address** — Specifies the IP address of the host (targeted recipient).
- **hostname** — Specifies the name of the host. (Range: 1-158 characters)
- **community-string** — Specifies a password-like community string sent with the notification operation. (Range: 1-20)
- **traps** — Indicates that SNMP traps are sent to this host. If unspecified, SNMPv2 traps are sent to the host.
- **informs** — Indicates that SNMP informs are sent to this host. Not applicable to SNMPv1.
- **1** — Indicates that SNMPv1 traps will be used.
- **2** — Indicates that SNMPv2 traps will be used.
- **port** — Specifies the UDP port of the host to use. If unspecified, the default UDP port number is 162. (Range: 1-65535)
- **filtername** — Specifies a string that defines the filter for this host. If unspecified, nothing is filtered. (Range: 1-30 characters)
- **seconds** — Specifies the number of seconds to wait for an acknowledgment before resending informs. If unspecified, the default timeout period is 15 seconds. (Range: 1-300)
- **retries** — Specifies the maximum number of times to resend an inform request. If unspecified, the default maximum number of retries is 3. (Range: 1-255)

**Default Setting**

This command has no default configuration.

**Command Mode**

Global Configuration mode

**Command Usage**

When configuring an SNMPv1 or SNMPv2 notification recipient, a notification view for that recipient is automatically generated for all the MIB.

When configuring an SNMPv1 notification recipient, the **Informs** option cannot be selected.

If a trap and inform are defined on the same target, and an inform was sent, the trap is not sent.
**Example**

The following command enables SNMP traps for host 10.1.1.1 with community string “management” using SNMPv2.

```
Console(config)# snmp-server host 10.1.1.1 management 2
```
The `snmp-server v3-host` Global Configuration mode command specifies the recipient of Simple Network Management Protocol Version 3 notifications. To remove the specified host, use the `no` form of this command.

**Syntax**

```plaintext
snmp-server v3-host {ip-address | hostname} username [traps | informs] {noauth | auth | priv} [udp-port port] [filter filtername] [timeout seconds] [retries retries]
```

**Parameters**

- **ip-address** — Specifies the IP address of the host (targeted recipient).
- **hostname** — Specifies the name of the host. (Range: 1-158 characters)
- **username** — Specifies the name of the user to use to generate the notification. (Range: 1-25)
- **traps** — Indicates that SNMP traps are sent to this host.
- **informs** — Indicates that SNMP informs are sent to this host.
- **noauth** — Indicates no authentication of a packet.
- **auth** — Indicates authentication of a packet without encrypting it.
- **priv** — Indicates authentication of a packet with encryption.
- **port** — Specifies the UDP port of the host to use. If unspecified, the default UDP port number is 162. (Range: 1-65535)
- **filtername** — Specifies a string that defines the filter for this host. If unspecified, nothing is filtered. (Range: 1-30 characters)
- **seconds** — Specifies the number of seconds to wait for an acknowledgment before resending informs. If unspecified, the default timeout period is 15 seconds. (Range: 1-300)
- **retries** — Specifies the maximum number of times to resend an inform request. If unspecified, the default maximum number of retries is 3. (Range: 1-255)

**Default Setting**

This command has no default configuration.

**Command Mode**

Global Configuration mode

**Command Usage**

A user and notification view are not automatically created. Use the `snmp-server user`, `snmp-server group` and `snmp-server view` Global Configuration mode commands to generate a user, group and notify group, respectively.

**Example**

The following command configures an SNMPv3 host.

```
Console(config)# snmp-server v3-host 192.168.0.20 john noauth
```
**snmp-server trap authentication**

The `snmp-server trap authentication` Global Configuration mode command enables the device to send SNMP traps when authentication fails. To disable SNMP failed authentication traps, use the `no` form of this command.

**Syntax**

`snmp-server trap authentication`

`no snmp-server trap authentication`

**Parameters**

There are no parameters for this command.

**Default Setting**

SNMP failed authentication traps are enabled.

**Command Mode**

Global Configuration mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command enables SNMP failed authentication traps.

```
Console(config)# snmp-server trap authentication
```
snmp-server contact

The snmp-server contact Global Configuration mode command configures the system contact (sysContact) string. To remove system contact information, use the no form of the command.

Syntax

snmp-server contact text
no snmp-server contact

Parameters

- text — Specifies the string that describes system contact information.
  (Range: 0-160 characters)

Default Setting

This command has no default configuration.

Command Mode

Global Configuration mode

Command Usage

Do not include spaces in the text string or place text that includes spaces inside quotation marks.

Example

The following command configures the system contact point called HP_Technical_Support.

```
Console(config)# snmp-server contact HP_Technical_Support
```
snmp-server location

The **snmp-server location** Global Configuration mode command configures the system location string. To remove the location string, use the **no** form of this command.

**Syntax**

```
snmp-server location text
no snmp-server location
```

**Parameters**

- `text` — Specifies a string that describes system location information. (Range: 0-160 characters)

**Default Setting**

This command has no default configuration.

**Command Mode**

Global Configuration mode

**Command Usage**

Do not include spaces in the text string or place text that includes spaces inside quotation marks.

**Example**

The following command defines the device location as **New_York**.

```
Console(config)# snmp-server location New_York
```
**snmp-server set**

The `snmp-server set` Global Configuration mode command defines the SNMP MIB value.

**Syntax**

```
(snmp-server set variable-name name1 value1 [ name2 value2 ...])
```

**Parameters**

- `variable-name` — MIB variable name.
- `name value` — List of name and value pairs. In the case of scalar MIBs, only a single pair of name values. In the case of an entry in a table, at least one pair of name and value followed by one or more fields.

**Default Setting**

This command has no default configuration.

**Command Mode**

Global Configuration mode

**Command Usage**

Although the CLI can set any required configuration, there might be a situation where a SNMP user sets a MIB variable that does not have an equivalent command. In order to generate configuration files that support those situations, the `snmp-server set` command is used.

This command is case-sensitive.

**Example**

The following command configures the scalar MIB sysName with the value HP.

```
Console(config)# snmp-server set sysName sysname HP
```
**show snmp**

The `show snmp` Privileged EXEC mode command displays the SNMP status.

**Syntax**

```
show snmp
```

**Parameters**

There are no parameters for this command.

**Default Setting**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command displays the SNMP communications status.

```
Console# show snmp

<table>
<thead>
<tr>
<th>Community-String</th>
<th>Community-Access</th>
<th>View Name</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>public</td>
<td>read only</td>
<td>user-view</td>
<td>All</td>
</tr>
<tr>
<td>private</td>
<td>read write</td>
<td>Default</td>
<td>172.16.1.1</td>
</tr>
<tr>
<td>private</td>
<td>su</td>
<td>DefaultSuper</td>
<td>172.17.1.1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Community-string</th>
<th>Group Name</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>public</td>
<td>user-group</td>
<td>all</td>
</tr>
</tbody>
</table>

Traps are enabled.
Authentication trap is enabled.

Version 1,2 notifications

<table>
<thead>
<tr>
<th>Target Address</th>
<th>Type</th>
<th>Community</th>
<th>Version</th>
<th>UDP Port</th>
<th>Filter Name</th>
<th>To Sec</th>
<th>Retries</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.122.173.42</td>
<td>Trap</td>
<td>public</td>
<td>2</td>
<td>162</td>
<td></td>
<td>15</td>
<td>3</td>
</tr>
<tr>
<td>192.122.173.42</td>
<td>Inform</td>
<td>public</td>
<td>2</td>
<td>162</td>
<td></td>
<td>15</td>
<td>3</td>
</tr>
</tbody>
</table>
The following table describes significant fields shown in the example.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Community-string</td>
<td>Community access string to permit access to the SNMP protocol.</td>
</tr>
<tr>
<td>Community-access</td>
<td>Type of access - read-only, read-write, super access.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Management station IP address.</td>
</tr>
<tr>
<td>Version</td>
<td>SNMP version for the sent trap 1 or 2.</td>
</tr>
</tbody>
</table>
show snmp engineid

The show snmp engineid Privileged EXEC mode command displays the ID of the local Simple Network Management Protocol (SNMP) engine.

Syntax

show snmp engineid

Parameters

There are no parameters for this command.

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following command displays the SNMP engine ID.

```
Console# show snmp engineid
Local SNMP engineid: 08009009020C0B099C075878
```
**show snmp views**

The `show snmp views` privileged EXEC mode command displays the configuration of views.

**Syntax**

`show snmp views [viewname]`

**Parameters**

- `viewname` — Specifies the name of the view. (Range: 1-30)

**Default Setting**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command displays the configuration of views.

```
Console# show snmp views

<table>
<thead>
<tr>
<th>Name</th>
<th>OID Tree</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>user-view</td>
<td>1.3.6.1.2.1.1</td>
<td>Included</td>
</tr>
<tr>
<td>user-view</td>
<td>1.3.6.1.2.1.1.7</td>
<td>Excluded</td>
</tr>
<tr>
<td>user-view</td>
<td>1.3.6.1.2.1.2.2.1.*.1</td>
<td>Included</td>
</tr>
</tbody>
</table>
```
show snmp groups

The show snmp groups Privileged EXEC mode command displays the configuration of groups.

Syntax

show snmp groups [groupname]

Parameters

- groupname — Specifies the name of the group. (Range: 1-30)

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following command displays the configuration of views.

```
Console# show snmp groups

<table>
<thead>
<tr>
<th>Name</th>
<th>Security</th>
<th>Level</th>
<th>Views</th>
<th>Write</th>
<th>Notify</th>
</tr>
</thead>
<tbody>
<tr>
<td>user-group</td>
<td>V3</td>
<td>priv</td>
<td>Default</td>
<td>***</td>
<td>==</td>
</tr>
<tr>
<td>managers-group</td>
<td>V3</td>
<td>priv</td>
<td>Default</td>
<td></td>
<td>==</td>
</tr>
<tr>
<td>managers-group</td>
<td>V3</td>
<td>priv</td>
<td>Default</td>
<td>***</td>
<td>==</td>
</tr>
</tbody>
</table>
```

The following table describes significant fields shown in the example.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the group.</td>
</tr>
<tr>
<td>Security</td>
<td>SNMP model in use (v1, v2 or v3).</td>
</tr>
<tr>
<td>Security Level</td>
<td>Authentication of a packet with encryption. Applicable only to the SNMP v3 security model.</td>
</tr>
<tr>
<td>Views Read</td>
<td>Name of the view that enables only viewing the contents of the agent. If unspecified, all objects except the community-table and SNMPv3 user and access tables are available.</td>
</tr>
<tr>
<td>Write</td>
<td>Name of the view that enables entering data and managing the contents of the agent.</td>
</tr>
<tr>
<td>Notify</td>
<td>Name of the view that enables specifying an inform or a trap.</td>
</tr>
</tbody>
</table>
show snmp filters

The show snmp filters Privileged EXEC mode command displays the configuration of filters.

Syntax

show snmp filters [filtername]

Parameters

- filtername — Specifies the name of the filter. (Range: 1-30)

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following command displays the configuration of filters.

```
Console# show snmp filters

<table>
<thead>
<tr>
<th>Name</th>
<th>OID Tree</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>user-filter</td>
<td>1.3.6.1.2.1.1</td>
<td>Included</td>
</tr>
<tr>
<td>user-filter</td>
<td>1.3.6.1.2.1.1.7</td>
<td>Excluded</td>
</tr>
<tr>
<td>user-filter</td>
<td>1.3.6.1.2.1.2.1.*.1</td>
<td>Included</td>
</tr>
</tbody>
</table>
```
**show snmp users**

The `show snmp users` Privileged EXEC mode command displays the configuration of users.

**Syntax**

```
show snmp users [username]
```

**Parameters**

- `username` — Specifies the name of the user. (Range: 1-30)

**Default Setting**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command displays the configuration of users.

```
Console# show snmp users

Name Group Name Auth Method Remote
------ ------------ -------- - -------------------------
John user-group md5 08009009020C0B099C075879
John user-group md5 08009009020C0B099C075879
```
spanning-tree

The `spanning-tree` Global Configuration mode command enables spanning-tree functionality. To disable spanning-tree functionality, use the `no` form of this command.

**Syntax**

```plaintext
spanning-tree
no spanning-tree
```

**Parameters**

There are no parameters for this command.

**Default Setting**

Spanning-tree is enabled. The MSTP-RSTP conversion parameter is enabled, which maps VLAN 1 to instance 1 and VLAN 2 to instance 2. This default provides interoperability with PVST/PVST+ by treating each MSTP instance as a separate spanning tree using standard RSTP and STP BPDUs.

**Command Modes**

Global Configuration mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command enables spanning-tree functionality.

```plaintext
Console(config)# spanning-tree
```
**spanning-tree mode**

The **spanning-tree mode** Global Configuration mode command configures the spanning-tree protocol. To return to the default configuration, use the **no** form of this command.

**Syntax**

```
spanning-tree mode {stp | rstp | mstp}
no spanning-tree mode
```

**Parameters**

- **stp** — Indicates that the Spanning Tree Protocol (STP) is enabled.
- **rstp** — Indicates that the Rapid Spanning Tree Protocol (RSTP) is enabled.
- **mstp** — Indicates that the Multiple Spanning Tree Protocol (RSTP) is enabled.

**Default Setting**

STP is enabled.

**Command Modes**

Global Configuration mode

**Command Usage**

In RSTP mode, the device uses STP when the neighbor device uses STP.

In MSTP mode, the device uses RSTP when the neighbor device uses RSTP and uses STP when the neighbor device uses STP.

**Example**

The following command configures the spanning-tree protocol to RSTP.

```
Console(config)# spanning-tree mode rstp
```
spanning-tree forward-time

The *spanning-tree forward-time* Global Configuration mode command configures the spanning-tree bridge forward time, which is the amount of time a port remains in the listening and learning states before entering the forwarding state. To return to the default configuration, use the *no* form of this command.

**Syntax**

`spanning-tree forward-time seconds`

`no spanning-tree forward-time`

**Parameters**

- `seconds` — Time in seconds. (Range: 4-30)

**Default Setting**

The default forwarding time for the IEEE Spanning Tree Protocol (STP) is 15 seconds.

**Command Modes**

Global Configuration mode

**Command Usage**

When configuring the forwarding time, the following relationship should be kept:

\[ 2 \times (\text{Forward-Time} - 1) \geq \text{Max-Age} \]

**Example**

The following command configures the spanning tree bridge forwarding time to 25 seconds.

```
Console(config)# spanning-tree forward-time 25
```
spanning-tree hello-time

The `spanning-tree hello-time` Global Configuration mode command configures the spanning tree bridge hello time, which is how often the device broadcasts hello messages to other devices. To return to the default configuration, use the `no` form of this command.

**Syntax**

```
spanning-tree hello-time seconds
no spanning-tree hello-time
```

**Parameters**

- `seconds` — Time in seconds. (Range: 1-10)

**Default Setting**

The default hello time for IEEE Spanning Tree Protocol (STP) is 2 seconds.

**Command Modes**

Global Configuration mode

**Command Usage**

When configuring the hello time, the following relationship should be kept:

Max-Age $\geq 2 \times$ (Hello-Time + 1)

**Example**

The following command configures spanning tree bridge hello time to 5 seconds.

```
Console(config)# spanning-tree hello-time 5
```
spanning-tree max-age

The `spanning-tree max-age` Global Configuration mode command configures the spanning tree bridge maximum age. To return to the default configuration, use the `no` form of this command.

**Syntax**

```
spanning-tree max-age seconds
no spanning-tree max-age
```

**Parameters**

- `seconds` — Time in seconds. (Range: 6-40)

**Default Setting**

The default maximum age for IEEE Spanning Tree Protocol (STP) is 20 seconds.

**Command Modes**

Global Configuration mode

**Command Usage**

When configuring the maximum age, the following relationships should be kept:

\[ 2 \times (\text{Forward-Time} - 1) \geq \text{Max-Age} \]

\[ \text{Max-Age} \geq 2 \times (\text{Hello-Time} + 1) \]

**Example**

The following command configures the spanning tree bridge maximum-age to 10 seconds.

```
Console(config)# spanning-tree max-age 10
```
spanning-tree priority

The `spanning-tree priority` Global Configuration mode command configures the spanning tree priority of the device. The priority value is used to determine which bridge is elected as the root bridge. To return to the default configuration, use the `no` form of this command.

**Syntax**

```
spanning-tree priority priority
do spanning-tree priority
```

**Parameters**

- `priority` — Priority of the bridge. (Range: 0-61440 in steps of 4096)

**Default Setting**

The default bridge priority for IEEE Spanning Tree Protocol (STP) is 32768.

**Command Modes**

Global Configuration mode

**Command Usage**

The bridge with the lowest priority is elected as the root bridge.

**Example**

The following command configures spanning tree priority to 12288.

```
Console(config)# spanning-tree priority 12288
```
spanning-tree disable

The `spanning-tree disable` Interface Configuration mode command disables spanning tree on a specific port. To enable spanning tree on a port, use the `no` form of this command.

**Syntax**

spanning-tree disable

no spanning-tree disable

**Parameters**

There are no parameters for this command.

**Default Setting**

Spanning tree is enabled on all ports.

**Command Modes**

Interface Configuration (Ethernet, port-channel) mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command disables spanning-tree on Ethernet port 1/e5.

```
Console(config)# interface ethernet 1/e5
Console(config-if)# spanning-tree disable
```
spanning-tree cost

The spanning-tree cost Interface Configuration mode command configures the spanning tree path cost for a port. To return to the default configuration, use the no form of this command.

Syntax

spanning-tree cost cost
no spanning-tree cost

Parameters

- cost — Path cost of the port (Range: 1 - 200,000,000)

Default Setting

Default path cost is determined by port speed and path cost method (long or short) as shown in the following table:

<table>
<thead>
<tr>
<th>Interface</th>
<th>Long</th>
<th>Short</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port-channel</td>
<td>20,000</td>
<td>4</td>
</tr>
<tr>
<td>Gigabit Ethernet (1000 Mbps)</td>
<td>20,000</td>
<td>4</td>
</tr>
<tr>
<td>Fast Ethernet (100 Mbps)</td>
<td>200,000</td>
<td>19</td>
</tr>
<tr>
<td>Ethernet (10 Mbps)</td>
<td>2,000,000</td>
<td>100</td>
</tr>
</tbody>
</table>

Command Modes

Interface Configuration (Ethernet, port-channel) mode

Command Usage

The path cost method is configured using the spanning-tree pathcost method Global Configuration mode command.

Example

The following command configures the spanning-tree cost on Ethernet port 1/e15 to 35000.

```
Console(config)# interface ethernet 1/e15
Console(config-if)# spanning-tree cost 35000
```
spanning-tree port-priority

The **spanning-tree port-priority** Interface Configuration mode command configures port priority. To return to the default configuration, use the **no** form of this command.

**Syntax**

```
spanning-tree port-priority priority
no spanning-tree port-priority
```

**Parameters**

- **priority** — The priority of the port. (Range: 0-240 in multiples of 16)

**Default Setting**

The default port priority for IEEE Spanning Tree Protocol (STP) is 128.

**Command Modes**

Interface Configuration (Ethernet, port-channel) mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command configures the spanning priority on Ethernet port 1/e15 to 96.

```
Console(config)# interface ethernet 1/e15
Console(config-if)# spanning-tree port-priority 96
```
spanning-tree portfast

The **spanning-tree portfast** Interface Configuration mode command enables PortFast mode. In PortFast mode, the interface is immediately put into the forwarding state upon linkup without waiting for the standard forward time delay. To disable PortFast mode, use the **no** form of this command.

**Syntax**

```
spanning-tree portfast [auto]
no spanning-tree portfast
```

**Parameters**

- **auto** — Specifies that the software waits for 3 seconds (with no BPDUs received on the interface) before putting the interface into PortFast mode.

**Default Setting**

PortFast mode is disabled.

**Command Modes**

Interface Configuration (Ethernet, port-channel) mode

**Command Usage**

This feature should be used only with interfaces connected to end stations. Otherwise, an accidental topology loop could cause a data packet loop and disrupt device and network operations.

An interface with PortFast mode enabled is moved directly to the spanning tree forwarding state when linkup occurs without waiting the standard forward-time delay.

**Example**

The following command enables PortFast on Ethernet port 1/e15.

```
Console(config)# interface ethernet 1/e15
Console(config-if)# spanning-tree portfast
```
spanning-tree link-type

The **spanning-tree link-type** Interface Configuration mode command overrides the default link-type setting determined by the duplex mode of the port and enables Rapid Spanning Tree Protocol (RSTP) transitions to the forwarding state. To return to the default configuration, use the **no** form of this command.

**Syntax**

```plaintext
spanning-tree link-type {point-to-point | shared}
no spanning-tree link-type
```

**Parameters**

- **point-to-point** — Indicates that the port link type is point-to-point.
- **shared** — Indicates that the port link type is shared.

**Default Setting**

The device derives the port link type from the duplex mode. A full-duplex port is considered a point-to-point link and a half-duplex port is considered a shared link.

**Command Modes**

Interface Configuration (Ethernet, port-channel) mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command enables shared spanning-tree on Ethernet port 1/e5.

```
Console(config)# interface ethernet 1/e5
Console(config-if)# spanning-tree link-type shared
```
spanning-tree pathcost method

The spanning-tree pathcost method Global Configuration mode command sets the default path cost method. To return to the default configuration, use the no form of this command.

Syntax

spanning-tree pathcost method {long | short}
no spanning-tree pathcost method

Parameters

- **long** — Specifies port path costs with a range of 1-200,000,000.
- **short** — Specifies port path costs with a range of 0-65,535.

Default Setting

Short path cost method.

Command Mode

Global Configuration mode

Command Usage

This command applies to all spanning tree instances on the device.

The cost is set using the spanning-tree cost command.

Example

The following command sets the default path cost method to long.

```
Console(config)# spanning-tree pathcost method long
```
spanning-tree bpdu

The `spanning-tree bpdu` Global Configuration mode command defines BPDU handling when the spanning tree is disabled globally or on a single interface. To return to the default configuration, use the `no` form of this command.

**Syntax**

`spanning-tree bpdu {filtering | flooding}`

**Parameters**

- **filtering** — Filter BPDU packets when the spanning tree is disabled on an interface.
- **flooding** — Flood BPDU packets when the spanning tree is disabled on an interface.

**Default Setting**

The default setting is flooding.

**Command Modes**

Global Configuration mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command defines BPDU packet flooding when the spanning-tree is disabled on an interface.

```
Console(config)# spanning-tree bpdu flooding
```
clear spanning-tree detected-protocols

The clear spanning-tree detected-protocols Privileged EXEC mode command restarts the protocol migration process (forces renegotiation with neighboring devices) on all interfaces or on a specified interface.

Syntax

```
clear spanning-tree detected-protocols [ethernet interface | port-channel port-channel-number]
```

Parameters

- **interface** — A valid Ethernet port.
- **port-channel-number** — A valid port-channel number.

Default Setting

This command has no default configuration.

Command Modes

Privileged EXEC mode

Command Usage

This feature should be used only when working in RSTP or MSTP mode.

Example

The following command restarts the protocol migration process on Ethernet port 1/e11.

```
Console# clear spanning-tree detected-protocols ethernet 1/e11
```
spanning-tree mst priority

The `spanning-tree mst priority` Global Configuration mode command configures the device priority for the specified spanning-tree instance. To return to the default configuration, use the `no` form of this command.

**Syntax**

```
spanning-tree mst instance-id priority priority
no spanning-tree mst instance-id priority
```

**Parameters**

- `instance-id` — ID of the spanning-tree instance (Range: 1-16).
- `priority` — Device priority for the specified spanning-tree instance (Range: 0-61440 in multiples of 4096).

**Default Setting**

The default bridge priority for IEEE Spanning Tree Protocol (STP) is 32768.

**Command Mode**

Global Configuration mode

**Command Usage**

The device with the lowest priority is selected as the root of the spanning tree.

**Example**

The following command configures the spanning tree priority of instance 1 to 4096.

```
console (config) # spanning-tree mst 1 priority 4096
```
spanning-tree mst max-hops

The `spanning-tree mst priority` Global Configuration mode command configures the number of hops in an MST region before the BDPU is discarded and the port information is aged out. To return to the default configuration, use the `no` form of this command.

**Syntax**

```
spanning-tree mst max-hops hop-count
no spanning-tree mst max-hops
```

**Parameters**

- `hop-count` — Number of hops in an MST region before the BDPU is discarded.
  (Range: 1-40)

**Default Setting**

The default number of hops is 20.

**Command Mode**

Global Configuration mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command configures the maximum number of hops that a packet travels in an MST region before it is discarded to 10.

```
console (config) # spanning-tree mst max-hops 10
```
spanning-tree mst port-priority

The `spanning-tree mst port-priority` Interface Configuration mode command configures port priority for the specified MST instance. To return to the default configuration, use the **no** form of this command.

**Syntax**

```plaintext
spanning-tree mst instance-id port-priority priority
no spanning-tree mst instance-id port-priority
```

**Parameters**

- `instance-ID` — ID of the spanning tree instance. (Range: 1-16)
- `priority` — The port priority. (Range: 0-240 in multiples of 16)

**Default Setting**

The default port priority for IEEE Multiple Spanning Tree Protocol (MSTP) is 128.

**Command Modes**

Interface Configuration (Ethernet, port-channel) mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command configures the port priority of port 1/g1 to 142.

```
Console(config)# interface ethernet 1/g1
Console(config-if)# spanning-tree mst 1 port-priority 142
```
spanning-tree mst cost

The `spanning-tree mst cost` Interface Configuration mode command configures the path cost for multiple spanning tree (MST) calculations. If a loop occurs, the spanning tree considers path cost when selecting an interface to put in the forwarding state. To return to the default configuration, use the `no` form of this command.

**Syntax**

```
spanning-tree mst instance-id cost cost
no spanning-tree mst instance-id cost
```

**Parameters**

- `instance-ID` — ID of the spanning-tree instance (Range: 1-16).
- `cost` — The port path cost. (Range: 1-200,000,000)

**Default Setting**

Default path cost is determined by port speed and path cost method (long or short) as shown in the following table:

<table>
<thead>
<tr>
<th>Interface</th>
<th>Long</th>
<th>Short</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port-channel</td>
<td>20,000</td>
<td>4</td>
</tr>
<tr>
<td>Gigabit Ethernet (1000 Mbps)</td>
<td>20,000</td>
<td>4</td>
</tr>
<tr>
<td>Fast Ethernet (100 Mbps)</td>
<td>200,000</td>
<td>19</td>
</tr>
<tr>
<td>Ethernet (10 Mbps)</td>
<td>2,000,000</td>
<td>100</td>
</tr>
</tbody>
</table>

**Command Modes**

Interface Configuration (Ethernet, port-channel) mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command configures the MSTP instance 1 path cost for Ethernet port 1/e9 to 4.

```
console(config) # interface ethernet 1/e9
console(config-if) # spanning-tree mst 1 cost 4
```
spanning-tree mst configuration

The `spanning-tree mst configuration` Global Configuration mode command enables configuring an MST region by entering the Multiple Spanning Tree (MST) mode.

Syntax

```plaintext
spanning-tree mst configuration
```

Parameters

There are no parameters for this command.

Default Setting

This command has no default configuration.

Command Mode

Global Configuration mode

Command Usage

All devices in an MST region must have the same VLAN mapping, configuration revision number and name.

Example

The following command configures an MST region.

```plaintext
Console(config)# spanning-tree mst configuration
console(config-mst)# instance 1 add vlan 10-20
console(config-mst)# name region1
console(config-mst)# revision 1
```
instance (mst)

The instance MST Configuration mode command maps VLANs to an MST instance.

Syntax

instance instance-id {add | remove} vlan vlan-range

Parameters

- instance-ID — ID of the MST instance (Range: 1-16).
- vlan-range — VLANs to be added to or removed from the specified MST instance. To specify a range of VLANs, use a hyphen. To specify a series of VLANs, use a comma. (Range: 1-4094).

Default Setting

VLANs are mapped to the common and internal spanning tree (CIST) instance (instance 0).

Command Modes

MST Configuration mode

Command Usage

All VLANs that are not explicitly mapped to an MST instance are mapped to the common and internal spanning tree (CIST) instance (instance 0) and cannot be unmapped from the CIST.

For two or more devices to be in the same MST region, they must have the same VLAN mapping, the same configuration revision number, and the same name.

Example

The following command maps VLANs 10-20 to MST instance 1.

```
Console(config)# spanning-tree mst configuration
console(config-mst)# instance 1 add vlan 10-20
```
name (mst)

The name MST Configuration mode command defines the configuration name. To return to the default setting, use the no form of this command.

Syntax

name string

Parameters

- string — MST configuration name. Case-sensitive (Range: 1-32 characters).

Default Setting

The default name is a bridge ID.

Command Mode

MST Configuration mode

Command Usage

There are no user guidelines for this command.

Example

The following command defines the configuration name as region1.

```
console(config) # spanning-tree mst configuration
console(config-mst) # name region 1
```
revision (mst)

The revision MST configuration command defines the configuration revision number. To return to the default configuration, use the no form of this command.

**Syntax**

```
revision value
no revision
```

**Parameters**

- **value** — Configuration revision number (Range: 0-65535).

**Default Setting**

The default configuration revision number is 0.

**Command Mode**

MST Configuration mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command sets the configuration revision to 1.

```
console(config) # spanning-tree mst configuration
console(config-mst) # revision 1
```
**show (mst)**

The `show MST` Configuration mode command displays the current or pending MST region configuration.

**Syntax**

`show {current | pending}`

**Parameters**

- **current** — Indicates the current region configuration.
- **pending** — Indicates the pending region configuration.

**Default Setting**

This command has no default configuration.

**Command Mode**

MST Configuration mode

**Command Usage**

The pending MST region configuration takes effect only after exiting the MST configuration mode.

**Example**

The following command displays a pending MST region configuration.

```
console(config-mst)# show pending

Pending MST configuration
Name: Region1
Revision: 1

<table>
<thead>
<tr>
<th>Instance</th>
<th>VLANs Mapped</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1-9,21-4094</td>
<td>Enabled</td>
</tr>
<tr>
<td>1</td>
<td>10-20</td>
<td>Enabled</td>
</tr>
</tbody>
</table>
```
exit (mst)

The `exit MST` Configuration mode command exits the MST configuration mode and applies all configuration changes.

**Syntax**

`exit`

**Parameters**

There are no parameters for this command.

**Default Setting**

This command has no default configuration.

**Command Mode**

MST Configuration mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command exits the MST configuration mode and saves changes.

```
console(config) # spanning-tree mst configuration
console(config-mst) # exit
```
**abort (mst)**

The `abort` MST Configuration mode command exits the MST configuration mode without applying the configuration changes.

**Syntax**

`abort`

**Parameters**

There are no parameters for this command.

**Default Setting**

This command has no default configuration.

**Command Mode**

MST Configuration mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command exits the MST configuration mode without saving changes.

```
console(config) # spanning-tree mst configuration
console(config-mst) # abort
```
spanning-tree guard root

The `spanning-tree guard root` Interface Configuration (Ethernet, port-channel) mode command enables root guard on all spanning tree instances on the interface. Root guard prevents the interface from becoming the root port of the device. To disable root guard on the interface, use the `no` form of this command.

**Syntax**

```
spanning-tree guard root
no spanning-tree guard root
```

**Parameters**

There are no parameters for this command.

**Default Setting**

Root guard is disabled.

**Command Mode**

Interface Configuration (Ethernet, port-channel) mode

**Command Usage**

Root guard can be enabled when the device operates in STP, RSTP, and MSTP.

When root guard is enabled, the port changes to the alternate state if spanning-tree calculations selects the port as the root port.

**Example**

The following command prevents Ethernet port 1/g1 from being the root port of the device.

```
console(config) # interface ethernet 1/g1
console(config-mst) # spanning-tree guard root
```
show spanning-tree

The show spanning-tree Privileged EXEC mode command displays spanning-tree configuration.

Syntax

```
show spanning-tree [ethernet interface -number| port-channel port-channel-number] [instance instance-id]
show spanning-tree [detail] [active | blockedports] [instance instance-id]
show spanning-tree mst-configuration
```

Parameters

- `interface -number` — A valid Ethernet port.
- `port-channel-number` — A valid port channel number.
- `detail` — Indicates detailed information.
- `active` — Indicates active ports only.
- `blockedports` — Indicates blocked ports only.
- `mst-configuration` — Indicates the MST configuration identifier.
- `instance-id` — Specifies ID of the spanning tree instance.

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following commands display spanning-tree information.

```
Console# show spanning-tree

Spanning tree enabled mode RSTP
Default port cost method: long

<table>
<thead>
<tr>
<th>Root ID</th>
<th>Priority</th>
<th>Address</th>
<th>Path Cost</th>
<th>Root Port</th>
<th>Hello Time 2 sec</th>
<th>Max Age 20 sec</th>
<th>Forward Delay 15 sec</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>32768</td>
<td>00:01:42:97:e0:00</td>
<td>20000</td>
<td>1 (1/e1)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```
### Spanning-Tree Commands

- **Bridge ID**
  - Priority: 36864
  - Address: 00:02:4b:29:7a:00
  - Hello Time: 2 sec
  - Max Age: 20 sec
  - Forward Delay: 15 sec

- **Interfaces**

<table>
<thead>
<tr>
<th>Name</th>
<th>State</th>
<th>Prio.Nbr</th>
<th>Cost</th>
<th>Sts</th>
<th>Role</th>
<th>PortFast</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/e1</td>
<td>Enabled</td>
<td>128.1</td>
<td>20000</td>
<td>FWD</td>
<td>Root</td>
<td>No</td>
<td>P2p (RSTP)</td>
</tr>
<tr>
<td>1/e2</td>
<td>Enabled</td>
<td>128.2</td>
<td>20000</td>
<td>FWD</td>
<td>Desg</td>
<td>No</td>
<td>Shared (STP)</td>
</tr>
<tr>
<td>1/e3</td>
<td>Disabled</td>
<td>128.3</td>
<td>20000</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>1/e4</td>
<td>Enabled</td>
<td>128.4</td>
<td>20000</td>
<td>BLK</td>
<td>ALTN</td>
<td>No</td>
<td>Shared (STP)</td>
</tr>
<tr>
<td>1/e5</td>
<td>Enabled</td>
<td>128.5</td>
<td>20000</td>
<td>DIS</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
</tbody>
</table>

---

```console
Console# show spanning-tree
```

Spanning tree enabled mode RSTP

Default port cost method: long

- **Root ID**
  - Priority: 36864
  - Address: 00:02:4b:29:7a:00

This switch is the root.

<table>
<thead>
<tr>
<th>Name</th>
<th>State</th>
<th>Prio.Nbr</th>
<th>Cost</th>
<th>Sts</th>
<th>Role</th>
<th>PortFast</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/e1</td>
<td>Enabled</td>
<td>128.1</td>
<td>20000</td>
<td>FWD</td>
<td>Desg</td>
<td>No</td>
<td>P2p (RSTP)</td>
</tr>
<tr>
<td>1/e2</td>
<td>Enabled</td>
<td>128.2</td>
<td>20000</td>
<td>FWD</td>
<td>Desg</td>
<td>No</td>
<td>Shared (STP)</td>
</tr>
<tr>
<td>1/e3</td>
<td>Disabled</td>
<td>128.3</td>
<td>20000</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>1/e4</td>
<td>Enabled</td>
<td>128.4</td>
<td>20000</td>
<td>FWD</td>
<td>Desg</td>
<td>No</td>
<td>Shared (STP)</td>
</tr>
<tr>
<td>1/e5</td>
<td>Enabled</td>
<td>128.5</td>
<td>20000</td>
<td>DIS</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
</tbody>
</table>
Spanning-Tree Commands

```markdown
Console# **show spanning-tree**

Spanning tree disabled (BPDU filtering) mode RSTP
Default port cost method: long

<table>
<thead>
<tr>
<th>Root ID</th>
<th>Priority</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Path Cost</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Root Port</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Hello Time</td>
<td>N/A</td>
<td>Max Age N/A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Bridge ID</th>
<th>Priority</th>
<th>36864</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>00:02:4b:29:7a:00</td>
<td></td>
</tr>
<tr>
<td>Hello Time 2 sec</td>
<td>Max Age 20 sec</td>
<td>Forward Delay 15 sec</td>
</tr>
</tbody>
</table>

**Interfaces**

<table>
<thead>
<tr>
<th>Name</th>
<th>State</th>
<th>Prio.Nbr</th>
<th>Cost</th>
<th>Sts</th>
<th>Role</th>
<th>PortFast</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/e1</td>
<td>Enabled</td>
<td>128.1</td>
<td>20000</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>1/e2</td>
<td>Enabled</td>
<td>128.2</td>
<td>20000</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>1/e3</td>
<td>Disabled</td>
<td>128.3</td>
<td>20000</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>1/e4</td>
<td>Enabled</td>
<td>128.4</td>
<td>20000</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>1/e5</td>
<td>Enabled</td>
<td>128.5</td>
<td>20000</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

Console# **show spanning-tree active**

Spanning tree enabled mode RSTP
Default port cost method: long

<table>
<thead>
<tr>
<th>Root ID</th>
<th>Priority</th>
<th>32768</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>00:01:42:97:e0:00</td>
<td></td>
</tr>
<tr>
<td>Path Cost</td>
<td>20000</td>
<td></td>
</tr>
<tr>
<td>Root Port</td>
<td>1 (1/e1)</td>
<td></td>
</tr>
<tr>
<td>Hello Time 2 sec</td>
<td>Max Age 20 sec</td>
<td>Forward Delay 15 sec</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Bridge ID</th>
<th>Priority</th>
<th>36864</th>
</tr>
</thead>
</table>
```

---

Spanning-Tree Commands

<table>
<thead>
<tr>
<th>Address</th>
<th>00:02:4b:29:7a:00</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hello Time 2 sec</td>
<td>Max Age 20 sec</td>
</tr>
<tr>
<td>Forward Delay 15 sec</td>
<td></td>
</tr>
</tbody>
</table>

**Interfaces**

<table>
<thead>
<tr>
<th>Name</th>
<th>State</th>
<th>Prio.Nbr</th>
<th>Cost</th>
<th>Sts</th>
<th>Role</th>
<th>PortFast</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/e1</td>
<td>Enabled</td>
<td>128.1</td>
<td>20000</td>
<td>FWD</td>
<td>Root</td>
<td>No</td>
<td>P2p (RSTP)</td>
</tr>
<tr>
<td>1/e2</td>
<td>Enabled</td>
<td>128.2</td>
<td>20000</td>
<td>FWD</td>
<td>Desg</td>
<td>No</td>
<td>Shared (STP)</td>
</tr>
<tr>
<td>1/e4</td>
<td>Enabled</td>
<td>128.4</td>
<td>20000</td>
<td>BLK</td>
<td>ALTN</td>
<td>No</td>
<td>Shared (STP)</td>
</tr>
</tbody>
</table>

**Console**

```
show spanning-tree blockedports
```

Spanning tree enabled mode RSTP

Default port cost method: long

<table>
<thead>
<tr>
<th>Root ID</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>00:01:42:97:e0:00</td>
</tr>
<tr>
<td>Path Cost</td>
<td>20000</td>
</tr>
<tr>
<td>Root Port</td>
<td>1 (1/1)</td>
</tr>
<tr>
<td>Hello Time 2 sec</td>
<td>Max Age 20 sec</td>
</tr>
<tr>
<td>Forward Delay 15 sec</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Bridge ID</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>00:02:4b:29:7a:00</td>
</tr>
<tr>
<td>Hello Time 2 sec</td>
<td>Max Age 20 sec</td>
</tr>
<tr>
<td>Forward Delay 15 sec</td>
<td></td>
</tr>
</tbody>
</table>

**Interfaces**

<table>
<thead>
<tr>
<th>Name</th>
<th>State</th>
<th>Prio.Nbr</th>
<th>Cost</th>
<th>Sts</th>
<th>Role</th>
<th>PortFast</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/e4</td>
<td>Enabled</td>
<td>128.4</td>
<td>20000</td>
<td>BLK</td>
<td>ALTN</td>
<td>No</td>
<td>Shared (STP)</td>
</tr>
</tbody>
</table>
Console# **show spanning-tree detail**

Spanning tree enabled mode RSTP
Default port cost method: long

<table>
<thead>
<tr>
<th>Root ID</th>
<th>Priority</th>
<th>32768</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td></td>
<td>00:01:42:97:e0:00</td>
</tr>
<tr>
<td>Path Cost</td>
<td></td>
<td>20000</td>
</tr>
<tr>
<td>Root Port</td>
<td></td>
<td>1 (1/e1)</td>
</tr>
<tr>
<td>Hello Time 2 sec</td>
<td></td>
<td>Max Age 20 sec</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Bridge ID</th>
<th>Priority</th>
<th>36864</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td></td>
<td>00:02:4b:29:7a:00</td>
</tr>
<tr>
<td>Hello Time 2 sec</td>
<td></td>
<td>Max Age 20 sec</td>
</tr>
</tbody>
</table>

Number of topology changes 2 last change occurred 2d18h ago
Times: hold 1, topology change 35, notification 2
       hello 2, max age 20, forward delay 15

Port 1 (1/e1) enabled
State: Forwarding Role: Root
Port id: 128.1 Port cost: 20000
Type: P2p (configured: auto) RSTP Port Fast: No (configured:no)
Designated bridge Priority: 32768 Address: 00:01:42:97:e0:00
Designated port id: 128.25 Designated path cost: 0
Number of transitions to forwarding state: 1
BPDU: sent 2, received 120638

Port 2 (1/e2) enabled
State: Forwarding Role: Designated
Port id: 128.2 Port cost: 20000
Type: Shared (configured: auto) STP Port Fast: No (configured:no)
Designated bridge Priority: 32768 Address: 00:02:4b:29:7a:00
Designated port id: 128.2 Designated path cost: 20000
Number of transitions to forwarding state: 1
BPDU: sent 2, received 170638
Spanning-Tree Commands

Port 3 (1/e3) disabled
State: N/A  Role: N/A
Port id: 128.3  Port cost: 20000
Type: N/A (configured: auto)  Port Fast: N/A (configured: no)
Designated bridge Priority: N/A  Address: N/A
Designated port id: N/A  Designated path cost: N/A
Number of transitions to forwarding state: N/A
BPDU: sent N/A, received N/A

Port 4 (1/e4) enabled
State: Blocking  Role: Alternate
Port id: 128.4  Port cost: 20000
Type: Shared (configured: auto) STP  Port Fast: No (configured: no)
Designated bridge Priority: 28672  Address: 00:30:94:41:62:c8
Designated port id: 128.25  Designated path cost: 20000
Number of transitions to forwarding state: 1
BPDU: sent 2, received 120638

Port 5 (1/e5) enabled
State: Disabled  Role: N/A
Port id: 128.5  Port cost: 20000
Type: N/A (configured: auto)  Port Fast: N/A (configured: no)
Designated bridge Priority: N/A  Address: N/A
Designated port id: N/A  Designated path cost: N/A
Number of transitions to forwarding state: N/A
BPDU: sent N/A, received N/A

Console# show spanning-tree ethernet 1/e1
Port 1 (1/e1) enabled
State: Forwarding  Role: Root
Port id: 128.1  Port cost: 20000
Type: P2p (configured: auto) RSTP  Port Fast: No (configured: no)
Designated bridge Priority: 32768  Address: 00:01:42:97:e0:00
Designated port id: 128.25  Designated path cost: 0
Number of transitions to forwarding state: 1
BPDU: sent 2, received 120638
Spanning-Tree Commands

### show spanning-tree mst-configuration

Name: Region1  
Revision: 1

<table>
<thead>
<tr>
<th>Instance</th>
<th>VLANs Mapped</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1-9, 21-4094</td>
<td>Enable</td>
</tr>
<tr>
<td>1</td>
<td>10-20</td>
<td>Enable</td>
</tr>
</tbody>
</table>

### show spanning-tree

Spanning tree enabled mode MSTP  
Default port cost method: long

#### MST 0 VLANs Mapped: 1-9, 21-4094

CST Root ID  
Priority: 32768  
Address: 00:01:42:97:e0:00  
Path Cost: 20000  
Root Port: 1 (1/e1)  
Hello Time: 2 sec  
Max Age: 20 sec  
Forward Delay: 15 sec

IST Master ID  
Priority: 32768  
Address: 00:02:4b:29:7a:00  
This switch is the IST master.  
Hello Time: 2 sec  
Max Age: 20 sec  
Forward Delay: 15 sec  
Max hops: 20

### Interfaces

<table>
<thead>
<tr>
<th>Name</th>
<th>State</th>
<th>Prio.Nbr</th>
<th>Cost</th>
<th>Sts</th>
<th>Role</th>
<th>PortFast</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/e1</td>
<td>Enabled</td>
<td>128.1</td>
<td>20000</td>
<td>FWD</td>
<td>Root</td>
<td>No</td>
<td>P2p Bound (RSTP)</td>
</tr>
<tr>
<td>1/e2</td>
<td>Enabled</td>
<td>128.2</td>
<td>20000</td>
<td>FWD</td>
<td>Desg</td>
<td>No</td>
<td>Shared Bound (STP)</td>
</tr>
<tr>
<td>1/e3</td>
<td>Enabled</td>
<td>128.3</td>
<td>20000</td>
<td>FWD</td>
<td>Desg</td>
<td>No</td>
<td>P2p</td>
</tr>
<tr>
<td>1/e4</td>
<td>Enabled</td>
<td>128.4</td>
<td>20000</td>
<td>FWD</td>
<td>Desg</td>
<td>No</td>
<td>P2p</td>
</tr>
</tbody>
</table>
### Spanning-Tree Commands

#### MST 1 VLANs Mapped: 10-20

<table>
<thead>
<tr>
<th>CST Root ID</th>
<th>Priority</th>
<th>Address</th>
<th>Path Cost</th>
<th>Root Port</th>
<th>Rem hops</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>00:02:4b:29:89:76</td>
<td>20000</td>
<td>4 (1/e4)</td>
<td>19</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CST Root ID</th>
<th>Priority</th>
<th>Address</th>
<th>Path Cost</th>
<th>Root Port</th>
<th>Rem hops</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>00:02:4b:29:7a:00</td>
<td>20000</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Interfaces

<table>
<thead>
<tr>
<th>Name</th>
<th>State</th>
<th>Prio.Nbr</th>
<th>Cost</th>
<th>Sts</th>
<th>Role</th>
<th>PortFast</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/e1</td>
<td>Enabled</td>
<td>128.1</td>
<td>20000</td>
<td>FWD</td>
<td>Boun</td>
<td>No</td>
<td>P2p Bound (RSTP)</td>
</tr>
<tr>
<td>1/e2</td>
<td>Enabled</td>
<td>128.2</td>
<td>20000</td>
<td>FWD</td>
<td>Boun</td>
<td>No</td>
<td>Shared Bound (STP)</td>
</tr>
<tr>
<td>1/e3</td>
<td>Enabled</td>
<td>128.3</td>
<td>20000</td>
<td>BLK</td>
<td>Altn</td>
<td>No</td>
<td>P2p</td>
</tr>
<tr>
<td>1/e4</td>
<td>Enabled</td>
<td>128.4</td>
<td>20000</td>
<td>FWD</td>
<td>Desg</td>
<td>No</td>
<td>P2p</td>
</tr>
</tbody>
</table>

Console# `show spanning-tree detail`

Spanning tree enabled mode MSTP
Default port cost method: long

#### MST 0 VLANs Mapped: 1-9, 21-4094

<table>
<thead>
<tr>
<th>CST Root ID</th>
<th>Priority</th>
<th>Address</th>
<th>Path Cost</th>
<th>Root Port</th>
<th>Hello Time 2 sec</th>
<th>Max Age 20 sec</th>
<th>Forward Delay 15 sec</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>00:01:42:97:e0:00</td>
<td>20000</td>
<td>1 (1/e1)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IST Master ID</th>
<th>Priority</th>
<th>Address</th>
<th>Max hops</th>
<th>Hello Time 2 sec</th>
<th>Max Age 20 sec</th>
<th>Forward Delay 15 sec</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>00:02:4b:29:7a:00</td>
<td>20</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

This switch is the IST master.

<table>
<thead>
<tr>
<th>IST Master ID</th>
<th>Priority</th>
<th>Address</th>
<th>Max hops</th>
<th>Hello Time 2 sec</th>
<th>Max Age 20 sec</th>
<th>Forward Delay 15 sec</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>00:02:4b:29:7a:00</td>
<td>20</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Number of topology changes 2 last change occurred 2d18h ago
Times: hold 1, topology change 35, notification 2
hello 2, max age 20, forward delay 15
<table>
<thead>
<tr>
<th>Port 1 (1/e1) enabled</th>
<th>Port 2 (1/e2) enabled</th>
<th>Port 3 (1/e3) enabled</th>
<th>Port 4 (1/e4) enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>State:</strong> Forwarding</td>
<td><strong>State:</strong> Forwarding</td>
<td><strong>State:</strong> Forwarding</td>
<td><strong>State:</strong> Forwarding</td>
</tr>
<tr>
<td><strong>Role:</strong> Root</td>
<td><strong>Role:</strong> Designated</td>
<td><strong>Role:</strong> Designated</td>
<td><strong>Role:</strong> Designated</td>
</tr>
<tr>
<td><strong>Port id:</strong> 128.1</td>
<td><strong>Port id:</strong> 128.2</td>
<td><strong>Port id:</strong> 128.3</td>
<td><strong>Port id:</strong> 128.4</td>
</tr>
<tr>
<td><strong>Type:</strong> P2p (configured: auto) Boundary RSTP</td>
<td><strong>Type:</strong> Shared (configured: auto) Boundary STP</td>
<td><strong>Type:</strong> Shared (configured: auto) Internal</td>
<td><strong>Type:</strong> Shared (configured: auto) Internal</td>
</tr>
<tr>
<td><strong>Designated bridge Priority:</strong> 32768</td>
<td><strong>Designated bridge Priority:</strong> 32768</td>
<td><strong>Designated bridge Priority:</strong> 32768</td>
<td><strong>Designated bridge Priority:</strong> 32768</td>
</tr>
<tr>
<td><strong>Designated port id:</strong> 128.25</td>
<td><strong>Designated port id:</strong> 128.2</td>
<td><strong>Designated port id:</strong> 128.3</td>
<td><strong>Designated port id:</strong> 128.2</td>
</tr>
<tr>
<td><strong>Number of transitions to forwarding state:</strong> 1</td>
<td><strong>Number of transitions to forwarding state:</strong> 1</td>
<td><strong>Number of transitions to forwarding state:</strong> 1</td>
<td><strong>Number of transitions to forwarding state:</strong> 1</td>
</tr>
<tr>
<td><strong>BPDU:</strong> sent 2, received 120638</td>
<td><strong>BPDU:</strong> sent 2, received 170638</td>
<td><strong>BPDU:</strong> sent 2, received 170638</td>
<td><strong>BPDU:</strong> sent 2, received 170638</td>
</tr>
</tbody>
</table>

### MST 1 VLANs Mapped: 10-20
### Spanning-Tree Commands

<table>
<thead>
<tr>
<th><strong>Root ID</strong></th>
<th><strong>Bridge ID</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
<td>Priority</td>
</tr>
<tr>
<td>24576</td>
<td>32768</td>
</tr>
<tr>
<td>Address</td>
<td>Address</td>
</tr>
<tr>
<td>00:02:4b:29:89:76</td>
<td>00:02:4b:29:7a:00</td>
</tr>
<tr>
<td>Path Cost</td>
<td>Path Cost</td>
</tr>
<tr>
<td>20000</td>
<td>20000</td>
</tr>
<tr>
<td>Port Cost</td>
<td>Port Cost</td>
</tr>
<tr>
<td>4 (1/e4)</td>
<td>20000</td>
</tr>
<tr>
<td>Rem hops</td>
<td>Times</td>
</tr>
<tr>
<td>19</td>
<td>hold 1, topology change 2, notification 2</td>
</tr>
</tbody>
</table>

**Times:**
- hold 1
- topology change 2
- notification 2
- hello 2, max age 20, forward delay 15

**Port 1 (1/e1) enabled**
- **State:** Forwarding
- **Role:** Boundary
- **Port id:** 128.1
- **Type:** P2p (configured: auto) Boundary RSTP
- **Designated bridge Priority:** 32768
- **Designated port id:** 128.1
- **Number of transitions to forwarding state:** 1
- **BPDU:** sent 2, received 120638

**Port 2 (1/e2) enabled**
- **State:** Forwarding
- **Role:** Designated
- **Port id:** 128.2
- **Type:** Shared (configured: auto) Boundary STP
- **Designated bridge Priority:** 32768
- **Designated port id:** 128.2
- **Number of transitions to forwarding state:** 1
- **BPDU:** sent 2, received 170638

**Port 3 (1/e3) disabled**
- **State:** Blocking
- **Role:** Alternate
- **Port id:** 128.3
- **Type:** Shared (configured: auto) Internal
- **Designated bridge Priority:** 32768
- **Designated port id:** 128.78
- **Number of transitions to forwarding state:** 1
- **BPDU:** sent 2, received 170638
Port 4 (1/e4) enabled
State: Forwarding Role: Designated
Port id: 128.4 Port cost: 20000
Type: Shared (configured: auto) Internal Port Fast: No (configured:no)
Designated bridge Priority: 32768 Address: 00:02:4b:29:7a:00
Designated port id: 128.2 Designated path cost: 20000
Number of transitions to forwarding state: 1
BPDU: sent 2, received 170638

Console# show spanning-tree

Spanning tree enabled mode MSTP
Default port cost method: long

#### MST 0 VLANs Mapped: 1-9, 21-4094

<table>
<thead>
<tr>
<th>CST Root ID</th>
<th>Priority</th>
<th>32768</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>00:01:42:97:e0:00</td>
<td></td>
</tr>
<tr>
<td>Path Cost</td>
<td>20000</td>
<td></td>
</tr>
<tr>
<td>Root Port</td>
<td>1 (1/e1)</td>
<td></td>
</tr>
<tr>
<td>Hello Time</td>
<td>2 sec</td>
<td></td>
</tr>
<tr>
<td>Max Age</td>
<td>20 sec</td>
<td></td>
</tr>
<tr>
<td>Forward Delay</td>
<td>15 sec</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IST Master ID</th>
<th>Priority</th>
<th>32768</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>00:02:4b:19:7a:00</td>
<td></td>
</tr>
<tr>
<td>Path Cost</td>
<td>10000</td>
<td></td>
</tr>
<tr>
<td>Rem hops</td>
<td>19</td>
<td></td>
</tr>
<tr>
<td>Hello Time</td>
<td>2 sec</td>
<td></td>
</tr>
<tr>
<td>Max Age</td>
<td>20 sec</td>
<td></td>
</tr>
<tr>
<td>Forward Delay</td>
<td>15 sec</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Bridge ID</th>
<th>Priority</th>
<th>32768</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>00:02:4b:29:7a:00</td>
<td></td>
</tr>
<tr>
<td>Hello Time</td>
<td>2 sec</td>
<td></td>
</tr>
<tr>
<td>Max Age</td>
<td>20 sec</td>
<td></td>
</tr>
<tr>
<td>Forward Delay</td>
<td>15 sec</td>
<td></td>
</tr>
</tbody>
</table>

Console# show spanning-tree

Spanning tree enabled mode MSTP
Default port cost method: long
### MST 0 VLANs Mapped: 1-9, 21-4094

<table>
<thead>
<tr>
<th>CST Root ID</th>
<th>Priority</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>32768</td>
<td>00:01:42:97:e0:00</td>
</tr>
</tbody>
</table>

This switch is root for CST and IST master.

<table>
<thead>
<tr>
<th>Root Port</th>
<th>Hello Time</th>
<th>Max Age</th>
<th>Forward Delay</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 (1/e1)</td>
<td>2 sec</td>
<td>20 sec</td>
<td>15 sec</td>
</tr>
</tbody>
</table>

Max hops 20
**spanning-tree pvst-interop**

The `spanning-tree pvst-interop` privileged EXEC command configures the device for PVST/PVST+ interoperability.

**Syntax**

`spanning-tree pvst-interop`

**Parameters**

This command has no arguments or keywords.

**Default Setting**

Disabled

**Command Modes**

Privileged EXEC

**Command Usage**

Before enabling this command the following is required:

- The port mode of all the ports in switch is set to Access.
- The number of VLANs in the switch is less than 16.

If there is a VLAN to MSTP mapping, the software asks the user to confirm that the existing mapping would be deleted.

This command performs the following:

- Enable MSTP.
- Map each VLAN to MSTP instance.
- Enable MSTP-to-STP conversion

The commands that shown in the startup-config, or running-config files, are the configuration commands executed by the script and not the command itself.

**Example**

The following command executes a script that configures the device for PVST/PVST+ interoperability.

```
Console# spanning-tree pvst-interop
```
spanning-tree mst mstp-rstp

The spanning-tree mst mstp-rstp interface configuration command configures the port to convert RSTP packets to MSTP instances. Use the no form of this command to disable the configuration.

Syntax

spanning-tree mst mstp-rstp
no spanning-tree mst mstp-rstp

Parameters

This command has no arguments or keywords.

Default Setting

Enabled.

Command Modes

Interface configuration (Ethernet, port-channel)

Command Usage

This mode can only be enabled in MSTP mode.

This is non-standard mode that enables the mapping of IEEE RSTP packets to MSTP instances as follows:

Incoming IEEE RSTP packets are mapped to the MSTP instance according to the default VLAN of the port.

The switch sends information through that port only for the instance of the default VLAN of that port. The information is sent in an IEEE RSTP packet with a bridge ID of the configured priority for that switch multiplied by 4096, plus the VLAN number of the default VLAN of the port, concatenated to the bridge MAC address.

If the port encounters a legacy STP BPDU on ingress, the conversion process will communicate with STP.

Example

The following command configures the port 1/e5 to convert RSTP packets to MSTP instances.

```
Console(config)# interface ethernet 1/e5
Console(config-if)# spanning-tree mst mstp-rstp
```
ip ssh port

The `ip ssh port` Global Configuration mode command specifies the port to be used by the SSH server. To return to the default configuration, use the `no` form of this command.

**Syntax**

```
ip ssh port port-number
no ip ssh port
```

**Parameters**

- `port-number` — Port number for use by the SSH server (Range: 1-65535).

**Default Setting**

The default port number is 22. SSH is disabled by default.

**Command Mode**

Global Configuration mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command specifies the port to be used by the SSH server as 8080.

```
Console(config)# ip ssh port 8080
```
**ip ssh server**

The **ip ssh server** Global Configuration mode command enables the device to be configured from a SSH server. To disable this function, use the **no** form of this command.

**Syntax**

*ip ssh server*

*no ip ssh server*

**Parameters**

There are no parameters for this command.

**Default Setting**

Device configuration from a SSH server is enabled. SSH is disabled by default.

**Command Mode**

Global Configuration mode

**Command Usage**

If encryption keys are not generated, the SSH server is in standby until the keys are generated. To generate SSH server keys, use the **crypto key generate dsa**, and **crypto key generate rsa** Global Configuration mode commands.

**Example**

The following command enables configuring the device from a SSH server.

```
Console(config)# ip ssh server
```
**crypto key generate dsa**

The *crypto key generate dsa* Global Configuration mode command generates DSA key pairs.

**Syntax**

`crypto key generate dsa`

**Parameters**

There are no parameters for this command.

**Default Setting**

DSA key pairs do not exist.

**Command Mode**

Global Configuration mode

**Command Usage**

DSA keys are generated in pairs: one public DSA key and one private DSA key. If the device already has DSA keys, a warning and prompt to replace the existing keys with new keys are displayed.

This command is not saved in the device configuration; however, the keys generated by this command are saved in the private configuration, which is never displayed to the user or backed up on another device.

DSA keys are saved to the backup master.

This command may take a considerable period of time to execute.

**Example**

The following command generates DSA key pairs.

```
Console(config)# crypto key generate dsa
```
**crypto key generate rsa**

The `crypto key generate rsa` Global Configuration mode command generates RSA key pairs.

**Syntax**

`crypto key generate rsa`

**Parameters**

There are no parameters for this command.

**Default Setting**

RSA key pairs do not exist.

**Command Mode**

Global Configuration mode

**Command Usage**

RSA keys are generated in pairs: one public RSA key and one private RSA key. If the device already has RSA keys, a warning and prompt to replace the existing keys with new keys are displayed.

This command is not saved in the device configuration; however, the keys generated by this command are saved in the private configuration which is never displayed to the user or backed up on another device.

RSA keys are saved to the backup master.

This command may take a considerable period of time to execute.

**Example**

The following command generates RSA key pairs.

```
Console(config)# crypto key generate rsa
```
ip ssh pubkey-auth

The `ip ssh pubkey-auth` Global Configuration mode command enables public key authentication for incoming SSH sessions. To disable this function, use the `no` form of this command.

**Syntax**

`ip ssh pubkey-auth`

`no ip ssh pubkey-auth`

**Parameters**

There are no parameters for this command.

**Default Setting**

Public Key authentication for incoming SSH sessions is disabled.

**Command Mode**

Global Configuration mode

**Command Usage**

AAA authentication is independent

**Example**

The following command enables public key authentication for incoming SSH sessions.

```console
Console(config)# ip ssh pubkey-auth
```
crypto key pubkey-chain ssh

The **crypto key pubkey-chain ssh** Global Configuration mode command enters the SSH Public Key-chain Configuration mode. The mode is used to manually specify other device public keys such as SSH client public keys.

**Syntax**

crypto key pubkey-chain ssh

**Parameters**

There are no parameters for this command.

**Default Setting**

No keys are specified.

**Command Mode**

Global Configuration mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following example shows how to enter the SSH Public Key-chain Configuration mode and manually configure the RSA key pair for SSH public key-chain *bob*.

```
Console(config)# crypto key pubkey-chain ssh
console(config-pubkey-chain)# user-key bob
console(config-pubkey-key)# key-string rsa
AAAAAB3NzaC1yc2EAAAADAQABAAABAQABAAABAQCVnRwPwI
Ai4kqplw9GBRnQZOxeHc/qK6rMIQ+
ZNXlZskvHG+QustZ/76ilMFT34v7u7ChFAE+
Vu4GrRfSwOvV35LqJK67O1U/ztf011g
kTwml75QR9gHujSo6KwGNZWxg3ub8gDjTSq
mu3n/Wo5lDx2E/xQwU081cqlk02LYCiz
+Z4TeU/9FrwP1VQ0jc+KBX10juNg5nFysY
OZC3nO/W9a/tnkm1shRE7D71+w3f9i0A
6w9o44f6+AINEICBCA4YC6zmzaT1wefWwX6f+
Rmt5nhqtdN1/0jPo166DqVXgWmN
zNR4DYVdSzg0IdmwCAC0qh

```
user-key

The user-key SSH Public Key-string Configuration mode command specifies which SSH public key is manually configured. To remove an SSH public key, use the no form of this command.

Syntax

user-key username {rsa | dsa}
no user-key username

Parameters

- username — Specifies the username of the remote SSH client. (Range: 1-48 characters)
- rsa — Indicates the RSA key pair.
- dsa — Indicates the DSA key pair.

Default Setting
No SSH public keys exist.

Command Mode
SSH Public Key-string Configuration mode

Command Usage

Follow this command with the key-string SSH Public Key-String Configuration mode command to specify the key.

Example

The following commands enable manually configuring an SSH public key for SSH public key-chain bob.

```
Console(config)# crypto key pubkey-chain ssh
console(config-pubkey-chain)# user-key bob rsa
console(config-pubkey-key)# key-string row
AAAAB3NzaC1yc2EAAAADAQABAAABAQA8AAAAABAAQAAAAQvTnTnW
```
key-string

The **key-string** SSH Public Key-string Configuration mode command manually specifies an SSH public key.

**Syntax**

```plaintext
key-string
key-string row key-string
```

**Parameters**

- **row** — Indicates the SSH public key row by row.
- **key-string** — Specifies the key in UU-encoded DER format; UU-encoded DER format is the same format in the authorized_keys file used by OpenSSH.

**Default Setting**

No keys exist.

**Command Mode**

SSH Public Key-string Configuration mode

**Command Usage**

Use the **key-string** SSH Public Key-string Configuration mode command to specify which SSH public key is to be interactively configured next. To complete the command, you must enter a row with no characters.

Use the **key-string row** SSH Public Key-string Configuration mode command to specify the SSH public key row by row. Each row must begin with a **key-string row** command. This command is useful for configuration files.
Example

The following command enters public key strings for SSH public key client **bob**.

```plaintext
Console(config)# crypto key pubkey-chain ssh
Console(config-pubkey-chain)# user-key bob rsa
Console(config-pubkey-key)# key-string
AAAAB3NzaC1yc2EAAAADAQABAAABAQCvTnRwPWIA
Al4kpqlw9GBRonZQZxjHKcqKL6rMIQ+
ZNXizSVkgHGQasz/76iLMF34v7u7ChFAE+
Vu4GRfpSwoQlVv35LqJjk67I0U/zfw011g
kTwmt75Q9S96rw3QGN2QWXgh3ub8gDjTSq
muSnWd0iDXz9ExWu08li3gk02LYciz
+Z4TrEU/9FJxwpIvOj+c+KBXuR0JnNg5nFysY
OZCkON/W9a/nkmlshRE7D71+w3fNIOA
6w9o44t6+AIIfICHCA4YcF6zMzaT1wenfWwX6f+
Rmt5nhqdaTI/40JFce166DqVX1gWmN
zNR4YDvSkg0DwNCAC8O0h


Console(config)# crypto key pubkey-chain ssh
Console(config-pubkey-chain)# user-key bob rsa
Console(config-pubkey-key)# key-string row AAAAB3Nza
Console(config-pubkey-key)# key-string row C1yc2
```
**show ip ssh**

The **show ip ssh** Privileged EXEC mode command displays the SSH server configuration.

**Syntax**

`show ip ssh`

**Parameters**

There are no parameters for this command.

**Default Setting**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command displays the SSH server configuration.

```
Console# show ip ssh

SSH server enabled. Port: 22
RSA key was generated.
DSA (DSS) key was generated.
SSH Public Key Authentication is enabled.
Active incoming sessions:

<table>
<thead>
<tr>
<th>IP Address</th>
<th>SSH username</th>
<th>Version</th>
<th>Cipher</th>
<th>Auth Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.0.1</td>
<td>John Brown</td>
<td>2.0</td>
<td>DES</td>
<td>HMAC-SHA1</td>
</tr>
</tbody>
</table>
```

The following table describes significant fields shown in the example.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>Client address</td>
</tr>
<tr>
<td>SSH username</td>
<td>User name</td>
</tr>
<tr>
<td>Version</td>
<td>SSH version number</td>
</tr>
<tr>
<td>Cipher</td>
<td>Encryption type (3DES, Blowfish, RC4)</td>
</tr>
<tr>
<td>Auth Code</td>
<td>Authentication Code (HMAC-MD5, HMAC-SHA1)</td>
</tr>
</tbody>
</table>
Syslog Commands

logging on

The `logging on` Global Configuration mode command controls error message logging. This command sends debug or error messages to a logging process, which logs messages to designated locations asynchronously to the process that generated the messages. To disable the logging process, use the `no` form of this command.

**Syntax**

logging on  
no logging on

**Parameters**

There are no parameters for this command.

**Default Setting**

Logging is enabled.

**Command Mode**

Global Configuration mode

**Command Usage**

The logging process controls the distribution of logging messages at various destinations, such as the logging buffer, logging file or syslog server. Logging on and off at these destinations can be individually configured using the `logging buffered`, `logging file`, and `logging` Global Configuration mode commands. However, if the `logging on` command is disabled, no messages are sent to these destinations. Only the console receives messages.

**Example**

The following command enables logging error messages.

```
Console(config)# logging on
```
Syslog Commands

logging

The **logging** Global Configuration mode command logs messages to a syslog server. To delete the syslog server with the specified address from the list of syslogs, use the **no** form of this command.

**Syntax**

```
logging {ip-address | hostname} [port port] [severity level] [facility facility] [description text]
no logging {ip-address | hostname}
```

**Parameters**

- **ip-address** — IP address of the host to be used as a syslog server.
- **hostname** — Specifies the host name of the syslog server. (Range: 1-158 characters)
- **port** — Specifies the port number for syslog messages. (Range: 1-65535)
- **level** — Specifies the severity level of logged messages sent to the syslog servers. Possible values: _emergencies_, _alerts_, _critical_, _errors_, _warnings_, _notifications_, _informational_ and _debugging_.
- **facility** — Specifies the facility that is indicated in the message. Possible values: _local0_, _local1_, _local2_, _local3_, _local4_, _local5_, _local6_, _local7_.
- **text** — Syslog server description. (Range: 1-64 characters)

**Default Setting**

The default port number is 514.
The default logging message level is _informational_.
The default facility is _local7_.

**Command Mode**

Global Configuration mode

**Command Usage**

Up to 8 syslog servers can be used.
If no severity level is specified, the global values apply to each server.

**Example**

The following command limits logged messages sent to the syslog server with IP address 10.1.1.1 to severity level _critical_.

```
Console(config)# logging 10.1.1.1 severity critical
```
logging console

The logging console Global Configuration mode command limits messages logged to the console based on severity. To disable logging to the console, use the no form of this command.

Syntax

logging console level

no logging console

Parameters

- level — Specifies the severity level of logged messages displayed on the console.
  Possible values: emergencies, alerts, critical, errors, warnings, notifications, informational and debugging.

Default Setting

The default severity level is informational.

Command Mode

Global Configuration mode

Command Usage

There are no user guidelines for this command.

Example

The following command limits logging messages displayed on the console to severity level errors.

```
Console(config)# logging console errors
```
logging buffered

The **logging buffered** Global Configuration mode command limits syslog messages displayed from an internal buffer based on severity. To cancel using the buffer, use the **no** form of this command.

**Syntax**

logging buffered *level*

no logging buffered

**Parameters**

- **level** — Specifies the severity level of messages logged in the buffer. Possible values: emergencies, alerts, critical, errors, warnings, notifications, informational and debugging.

**Default Setting**

The default severity level is informational.

**Command Mode**

Global Configuration mode

**Command Usage**

All the syslog messages are logged to the internal buffer. This command limits the messages displayed to the user.

**Example**

The following command limits syslog messages displayed from an internal buffer based on severity level **debugging**.

```
Console(config)# logging buffered debugging
```
**logging buffered size**

The `logging buffered size` Global Configuration mode command changes the number of syslog messages stored in the internal buffer. To return to the default configuration, use the `no` form of this command.

**Syntax**

```
logging buffered size number
no logging buffered size
```

**Parameters**

- `number` — Specifies the maximum number of messages stored in the history table.  
  (Range: 20–400)

**Default Setting**

The default number of messages is 200.

**Command Mode**

Global Configuration mode

**Command Usage**

This command takes effect only after Reset.

**Example**

The following command changes the number of syslog messages stored in the internal buffer to 300.

```
Console(config)# logging buffered size 300
```
clear logging

The `clear logging` Privileged EXEC mode command clears messages from the internal logging buffer.

**Syntax**

`clear logging`

**Parameters**

There are no parameters for this command.

**Default Setting**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command clears messages from the internal logging buffer.

```
Console# clear logging
Clear logging buffer [confirm]
```
logging file

The **logging file** Global Configuration mode command limits syslog messages sent to the logging file based on severity. To cancel using the buffer, use the **no** form of this command.

**Syntax**

```
logging file level
no logging file
```

**Parameters**

- **level** — Specifies the severity level of syslog messages sent to the logging file. Possible values: **emergencies, alerts, critical, errors, warnings, notifications, informational** and **debugging**.

**Default Setting**

The default severity level is **errors**.

**Command Mode**

Global Configuration mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command limits syslog messages sent to the logging file based on severity level **alerts**.

```
Console(config)# logging file alerts
```
**clear logging file**

The `clear logging file` Privileged EXEC mode command clears messages from the logging file.

**Syntax**

`clear logging file`

**Parameters**

There are no parameters for this command.

**Default Setting**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command clears messages from the logging file.

```
Console# clear logging file
Clear Logging File [confirm]
```
aaa logging

The **aaa logging** Global Configuration mode command enables logging AAA login events. To disable logging AAA login events, use the **no** form of this command.

**Syntax**

aaa logging login

no aaa logging login

**Parameters**

- **login** — Indicates logging messages related to successful login events, unsuccessful login events and other login-related events.

**Default Setting**

Logging AAA login events is enabled.

**Command Mode**

Global Configuration mode

**Command Usage**

Other types of AAA events are not subject to this command.

**Example**

The following command enables logging messages related to AAA login events.

```
Console(config)# aaa logging login
```
**file-system logging**

The **file-system logging** Global Configuration mode command enables logging file system events. To disable logging file system events, use the **no** form of this command.

**Syntax**

```
file-system logging copy
no file-system logging copy
file-system logging delete-rename
no file-system logging delete-rename
```

**Parameters**

- **copy** — Indicates logging messages related to file copy operations.
- **delete-rename** — Indicates logging messages related to file deletion and renaming operations.

**Default Setting**

Logging file system events is enabled.

**Command Mode**

Global Configuration mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command enables logging messages related to file copy operations.

```
Console(config)# file-system logging copy
```
management logging

The `management logging` global configuration command enables logging management access list (ACL) events. To disable logging management access list events, use the `no` form of this command.

**Syntax**

management logging deny

no management logging deny

**Parameters**

- `deny` — Indicates logging messages related to deny actions of management ACLs.

**Default Setting**

Logging management ACL events is enabled.

**Command Mode**

Global Configuration mode

**Command Usage**

Other types of management ACL events are not subject to this command.

**Example**

The following command enables logging messages related to deny actions of management ACLs.

```
Console(config)# management logging deny
```
show logging

The `show logging` Privileged EXEC mode command displays the state of logging and the syslog messages stored in the internal buffer.

**Syntax**

`show logging`

**Parameters**

There are no parameters for this command.

**Default Setting**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command displays the state of logging and the syslog messages stored in the internal buffer.

```
Console# show logging

Logging is enabled.
Console logging: level debugging. Console Messages: 0 Dropped (severity).
File logging: level notifications. File Messages: 0 Dropped (severity).
2 messages were not logged (resources)
Application filtering control

<table>
<thead>
<tr>
<th>Application</th>
<th>Event</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA</td>
<td>Login</td>
<td>Enabled</td>
</tr>
<tr>
<td>File system</td>
<td>Copy</td>
<td>Enabled</td>
</tr>
<tr>
<td>File system</td>
<td>Delete-Rename</td>
<td>Enabled</td>
</tr>
<tr>
<td>Management ACL</td>
<td>Deny</td>
<td>Enabled</td>
</tr>
</tbody>
</table>
```
### Syslog Commands

**Buffer log:**

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>11-Aug-04</td>
<td>15:41:43</td>
<td>%LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up</td>
</tr>
<tr>
<td>11-Aug-04</td>
<td>15:41:43</td>
<td>%LINK-3-UPDOWN: Interface Ethernet1/0, changed state to up</td>
</tr>
<tr>
<td>11-Aug-04</td>
<td>15:41:43</td>
<td>%LINK-3-UPDOWN: Interface Ethernet1/1, changed state to up</td>
</tr>
<tr>
<td>11-Aug-04</td>
<td>15:41:43</td>
<td>%LINK-3-UPDOWN: Interface Ethernet1/2, changed state to up</td>
</tr>
<tr>
<td>11-Aug-04</td>
<td>15:41:43</td>
<td>%LINK-3-UPDOWN: Interface Ethernet1/3, changed state to up</td>
</tr>
<tr>
<td>11-Aug-04</td>
<td>15:41:43</td>
<td>%SYS-5-CONFIG_I: Configured from memory by console</td>
</tr>
<tr>
<td>11-Aug-04</td>
<td>15:41:39</td>
<td>%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up</td>
</tr>
<tr>
<td>11-Aug-04</td>
<td>15:41:39</td>
<td>%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/0, changed state to down</td>
</tr>
<tr>
<td>11-Aug-04</td>
<td>15:41:39</td>
<td>%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/1, changed state to down</td>
</tr>
<tr>
<td>11-Aug-04</td>
<td>15:41:39</td>
<td>%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/2, changed state to down</td>
</tr>
<tr>
<td>11-Aug-04</td>
<td>15:41:39</td>
<td>%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/3, changed state to down</td>
</tr>
</tbody>
</table>
show logging file

The show logging file Privileged EXEC mode command displays the state of logging and the syslog messages stored in the logging file.

Syntax

show logging file

Parameters

There are no parameters for this command.

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following command displays the logging state and the syslog messages stored in the logging file.

```
Console# show logging file

Logging is enabled.
Console logging: level debugging. Console Messages: 0 Dropped (severity).
File logging: level notifications. File Messages: 0 Dropped (severity).
2 messages were not logged (resources)
Application filtering control

<table>
<thead>
<tr>
<th>Application</th>
<th>Event</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA</td>
<td>Login</td>
<td>Enabled</td>
</tr>
<tr>
<td>File system</td>
<td>Copy</td>
<td>Enabled</td>
</tr>
<tr>
<td>File system</td>
<td>Delete-Rename</td>
<td>Enabled</td>
</tr>
<tr>
<td>Management ACL</td>
<td>Deny</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

Buffer log:

11-Aug-2004 15:41:43: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
11-Aug-2004 15:41:43: %LINK-3-UPDOWN: Interface Ethernet1/0, changed state to up
11-Aug-2004 15:41:43: %LINK-3-UPDOWN: Interface Ethernet1/1, changed state to up
```
11-Aug-2004 15:41:43: %LINK-3-UPDOWN: Interface Ethernet1/2, changed state to up
11-Aug-2004 15:41:43: %LINK-3-UPDOWN: Interface Ethernet1/3, changed state to up
11-Aug-2004 15:41:43: %SYS-5-CONFIG_I: Configured from memory by console
11-Aug-2004 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
11-Aug-2004 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/0, changed state to down
11-Aug-2004 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/1, changed state to down
11-Aug-2004 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/2, changed state to down
System Management Commands

ping

The `ping` User EXEC mode command sends ICMP echo request packets to another node on the network.

**Syntax**

`ping {ip-address | hostname} [size packet_size] [count packet_count] [timeout time_out]`

**Parameters**

- `ip-address` — IP address to ping.
- `hostname` — Host name to ping. (Range: 1-158 characters)
- `packet_size` — Number of bytes in a packet. The actual packet size is eight bytes larger than the specified size specified because the device adds header information. (Range: 56-1472 bytes)
- `packet_count` — Number of packets to send. If 0 is entered, it pings until stopped. (Range: 0-65535 packets)
- `time_out` — Timeout in milliseconds to wait for each reply. (Range: 50 - 65535 milliseconds)

**Default Setting**

Default buffer size is 56 bytes.
Default number of packets to send is 4.
Default timeout value is 2000 milliseconds.

**Command Mode**

User EXEC mode

**Command Usage**

Press `Esc` to stop pinging.

Following are examples of unsuccessful pinging:

- `Destination does not respond` — If the host does not respond, a “no answer from host” appears in ten seconds.
- `Destination unreachable` — The gateway for this destination indicates that the destination is unreachable.
- `Network or host unreachable` — The device found no corresponding entry in the route table.
Example

The following command displays pinging results:

```
Console> ping 10.1.1.1

Pinging 10.1.1.1 with 64 bytes of data:

64 bytes from 10.1.1.1: icmp_seq=0. time=11 ms
64 bytes from 10.1.1.1: icmp_seq=1. time=8 ms
64 bytes from 10.1.1.1: icmp_seq=2. time=8 ms
64 bytes from 10.1.1.1: icmp_seq=3. time=7 ms

----10.1.1.1 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms) min/avg/max = 7/8/11

Console> ping yahoo.com

Pinging yahoo.com 66.218.71.198 with 64 bytes of data:

64 bytes from 10.1.1.1: icmp_seq=0. time=11 ms
64 bytes from 10.1.1.1: icmp_seq=1. time=8 ms
64 bytes from 10.1.1.1: icmp_seq=2. time=8 ms
64 bytes from 10.1.1.1: icmp_seq=3. time=7 ms

----10.1.1.1 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms) min/avg/max = 7/8/11
```
The **traceroute** User EXEC mode command discovers routes that packets actually take when traveling to their destination.

**Syntax**

```
traceroute {ip-address | hostname } [size packet_size] [ttl max-ttl] [count packet_count] [timeout time_out] [source ip-address] [tos tos]
```

**Parameters**

- **ip-address** — IP address of the destination host.
- **hostname** — Host name of the destination host. (Range: 1-158 characters)
- **packet_size** — Number of bytes in a packet. (Range: 40-1500)
- **max-ttl** — The largest TTL value that can be used. The **traceroute** command terminates when the destination is reached or when this value is reached. (Range: 1-255)
- **packet_count** — The number of probes to be sent at each TTL level. (Range: 1-10)
- **time_out** — The number of seconds to wait for a response to a probe packet. (Range: 1-60)
- **ip-address** — One of the device’s interface addresses to use as a source address for the probes. The device normally selects what it feels is the best source address to use.
- **tos** — The Type-Of-Service byte in the IP Header of the packet. (Range: 0-255)

**Default Setting**

The default number of bytes in a packet is 40.
The default maximum TTL value is 30.
The default number of probes to be sent at each TTL level is 3.
The default timeout interval in seconds is 3.

**Command Mode**

User EXEC mode

**Command Usage**

The **traceroute** command takes advantage of the error messages generated by the devices when a datagram exceeds its time-to-live (TTL) value.

The **traceroute** command starts by sending probe datagrams with a TTL value of one. This causes the first device to discard the probe datagram and send back an error message. The **traceroute** command sends several probes at each TTL level and displays the round-trip time for each.

The **traceroute** command sends out one probe at a time. Each outgoing packet may result in one or two error messages. A “time exceeded” error message indicates that an intermediate device has seen and discarded the probe. A “destination unreachable” error message indicates that the destination node has received the probe and discarded it because it could not deliver the packet. If the timer goes off before a response comes in, the **traceroute** command prints an asterisk (*).

The **traceroute** command terminates when the destination responds, when the maximum TTL is exceeded or when the user interrupts the trace by pressing **Esc**.
Examples

The following command discovers the routes that packets will actually take when traveling to their destination.

```
Console# traceroute 192.168.2.5

Tracing the route to 192.168.2.5 (192.168.2.5), 30 hops max, 40 byte packets
Type Esc to abort.
1 192.168.2.5 (192.168.2.5) <20 ms <20 ms <20 ms
Trace complete.
Console#
```

The following table describes significant fields shown in the example.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Indicates the sequence number of the device in the path to the host.</td>
</tr>
<tr>
<td>i2-gateway.stanford.edu</td>
<td>Host name of this device.</td>
</tr>
<tr>
<td>192.68.191.83</td>
<td>IP address of this device.</td>
</tr>
<tr>
<td>1 m sec 1 m sec 1 m sec</td>
<td>Round-trip time for each probe sent.</td>
</tr>
</tbody>
</table>

The following table describes characters that may appear in the `traceroute` command output.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>The probe timed out.</td>
</tr>
<tr>
<td>?</td>
<td>Unknown packet type.</td>
</tr>
<tr>
<td>A</td>
<td>Administratively unreachable. Usually, this output indicates that an access list is blocking traffic.</td>
</tr>
<tr>
<td>F</td>
<td>Fragmentation is required and DF is set.</td>
</tr>
<tr>
<td>H</td>
<td>Host unreachable.</td>
</tr>
<tr>
<td>N</td>
<td>Network unreachable.</td>
</tr>
<tr>
<td>P</td>
<td>Protocol unreachable.</td>
</tr>
<tr>
<td>Q</td>
<td>Source quench.</td>
</tr>
<tr>
<td>R</td>
<td>Fragment reassembly time exceeded.</td>
</tr>
<tr>
<td>S</td>
<td>Source route failed.</td>
</tr>
<tr>
<td>U</td>
<td>Port unreachable.</td>
</tr>
</tbody>
</table>
**telnet**

The `telnet` User EXEC mode command enables logging on to a host that supports Telnet.

**Syntax**

```
telnet {ip-address | hostname} [port] [keyword1......]
```

**Parameters**

- `ip-address` — IP address of the destination host.
- `hostname` — Host name of the destination host. (Range: 1-158 characters)
- `port` — A decimal TCP port number, or one of the keywords listed in the Ports table in the Command Usage.
- `keyword` — One or more keywords listed in the Keywords table in the Command Usage.

**Default Setting**

The default port is the Telnet port (decimal 23) on the host.

**Command Mode**

User EXEC mode

**Command Usage**

Telnet software supports special Telnet commands in the form of Telnet sequences that map generic terminal control functions to operating system-specific functions. To enter a Telnet sequence, press the escape sequence keys (Ctrl-shift-6) followed by a Telnet command character.

**Telnet Sequence**

<table>
<thead>
<tr>
<th>Telnet Sequence</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ctrl-shift-6-b</td>
<td>Break</td>
</tr>
<tr>
<td>Ctrl-shift-6-c</td>
<td>Interrupt Process (IP)</td>
</tr>
<tr>
<td>Ctrl-shift-6-h</td>
<td>Erase Character (EC)</td>
</tr>
<tr>
<td>Ctrl-shift-6-o</td>
<td>Abort Output (AO)</td>
</tr>
<tr>
<td>Ctrl-shift-6-t</td>
<td>Are You There? (AYT)</td>
</tr>
<tr>
<td>Ctrl-shift-6-u</td>
<td>Erase Line (EL)</td>
</tr>
</tbody>
</table>
At any time during an active Telnet session, Telnet commands can be listed by pressing the Ctrl-shift-6-? keys at the system prompt, as shown in the following example. Note that the Ctrl-shift-6 sequence appears as ^ on the screen.

```
Console> 'Ctrl-shift-6' ?

[Special telnet escape help]
^^ B sends telnet BREAK
^^ C sends telnet IP
^^ H sends telnet EC
^^ O sends telnet AO
^^ T sends telnet AYT
^^ U sends telnet EL
Ctrl-shift-6 x suspends the session (return to system command prompt)
```

Several concurrent Telnet sessions can be opened and switched. To open a subsequent session, the current connection has to be suspended by pressing the escape sequence keys (Ctrl-shift-6) and x to return to the system command prompt. Then open a new connection with the `telnet` User EXEC mode command.

### Keywords Table

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/echo</td>
<td>Enables local echo.</td>
</tr>
<tr>
<td>/quiet</td>
<td>Prevents on-screen display of all messages from the software.</td>
</tr>
<tr>
<td>/source-interface</td>
<td>Specifies the source interface.</td>
</tr>
<tr>
<td>/stream</td>
<td>Turns on stream processing, which enables a raw TCP stream with no Telnet control sequences. A stream connection does not process Telnet options and can be appropriate for connections to ports running UNIX-to-UNIX Copy Program (UUCP) and other non-Telnet protocols.</td>
</tr>
<tr>
<td>Ctrl-shift-6 x</td>
<td>Return to system command prompt.</td>
</tr>
</tbody>
</table>

### Ports Table

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
<th>Port Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP</td>
<td>Border Gateway Protocol</td>
<td>179</td>
</tr>
<tr>
<td>chargen</td>
<td>Character generator</td>
<td>19</td>
</tr>
<tr>
<td>cmd</td>
<td>Remote commands</td>
<td>514</td>
</tr>
<tr>
<td>daytime</td>
<td>Daytime</td>
<td>13</td>
</tr>
<tr>
<td>discard</td>
<td>Discard</td>
<td>9</td>
</tr>
<tr>
<td>domain</td>
<td>Domain Name Service</td>
<td>53</td>
</tr>
<tr>
<td>echo</td>
<td>Echo</td>
<td>7</td>
</tr>
<tr>
<td><strong>Keyword</strong></td>
<td><strong>Description</strong></td>
<td><strong>Port Number</strong></td>
</tr>
<tr>
<td>-------------</td>
<td>-----------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>exec</td>
<td>Exec</td>
<td>512</td>
</tr>
<tr>
<td>finger</td>
<td>Finger</td>
<td>79</td>
</tr>
<tr>
<td>ftp</td>
<td>File Transfer Protocol</td>
<td>21</td>
</tr>
<tr>
<td>ftp-data</td>
<td>FTP data connections</td>
<td>20</td>
</tr>
<tr>
<td>gopher</td>
<td>Gopher</td>
<td>70</td>
</tr>
<tr>
<td>hostname</td>
<td>NIC hostname server</td>
<td>101</td>
</tr>
<tr>
<td>ident</td>
<td>Ident Protocol</td>
<td>113</td>
</tr>
<tr>
<td>irc</td>
<td>Internet Relay Chat</td>
<td>194</td>
</tr>
<tr>
<td>klogin</td>
<td>Kerberos login</td>
<td>543</td>
</tr>
<tr>
<td>kshell</td>
<td>Kerberos shell</td>
<td>544</td>
</tr>
<tr>
<td>login</td>
<td>Login</td>
<td>513</td>
</tr>
<tr>
<td>lpd</td>
<td>Printer service</td>
<td>515</td>
</tr>
<tr>
<td>nntp</td>
<td>Network News Transport Protocol</td>
<td>119</td>
</tr>
<tr>
<td>pim-auto-rp</td>
<td>PIM Auto-RP</td>
<td>496</td>
</tr>
<tr>
<td>pop2</td>
<td>Post Office Protocol v2</td>
<td>109</td>
</tr>
<tr>
<td>pop3</td>
<td>Post Office Protocol v3</td>
<td>110</td>
</tr>
<tr>
<td>smtp</td>
<td>Simple Mail Transport Protocol</td>
<td>25</td>
</tr>
<tr>
<td>sunrpc</td>
<td>Sun Remote Procedure Call</td>
<td>111</td>
</tr>
<tr>
<td>syslog</td>
<td>Syslog</td>
<td>514</td>
</tr>
<tr>
<td>tacacs</td>
<td>TAC Access Control System</td>
<td>49</td>
</tr>
<tr>
<td>talk</td>
<td>Talk</td>
<td>517</td>
</tr>
<tr>
<td>telnet</td>
<td>Telnet</td>
<td>23</td>
</tr>
<tr>
<td>time</td>
<td>Time</td>
<td>37</td>
</tr>
<tr>
<td>uucp</td>
<td>Unix-to-Unix Copy Program</td>
<td>540</td>
</tr>
<tr>
<td>whois</td>
<td>Nickname</td>
<td>43</td>
</tr>
<tr>
<td>www</td>
<td>World Wide Web</td>
<td>80</td>
</tr>
</tbody>
</table>

This command lists concurrent Telnet connections to remote hosts that were opened by the current telnet session to the local device. It does not list Telnet connections to remote hosts that were opened by other Telnet sessions.

**Example**

The following command connects to 176.213.10.50 via Telnet.

```
Console> telnet 176.213.10.50
Esc U sends telnet EL
```
The **resume** User EXEC mode command enables switching to another open Telnet session.

### Syntax

```
resume [connection]
```

### Parameters

- **connection** — The connection number. (Range: 1-4 connections)

### Default Setting

The default connection number is that of the most recent connection.

### Command Mode

User EXEC mode

### Command Usage

There are no user guidelines for this command.

### Example

The following command switches to open Telnet session number 1.

```
Console> resume 1
```
**reload**

The `reload` Privileged EXEC mode command reloads the operating system.

**Syntax**

`reload`

**Parameters**

There are no parameters for this command.

**Default Setting**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode

**Command Usage**

Caution should be exercised when resetting the device, to ensure that no other activity is being performed. In particular, the user should verify that no configuration files are being downloaded at the time of reset.

**Example**

The following command reloads the operating system.

```
Console# reload
This command will reset the whole system and disconnect your current session. Do you want to continue (y/n) [n]?
```
hostname

The hostname Global Configuration mode command specifies or modifies the device host name. To remove the existing host name, use the no form of the command.

**Syntax**

hostname name
no hostname

**Parameters**

- **name** — The host name of the device. (Range: 1-158 characters)

**Default Setting**

This command has no default configuration.

**Command Mode**

Global Configuration mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command specifies the device host name.

```
Console(config)# hostname HP
HP(config)#
```
show users

The `show users` User EXEC mode command displays information about the active users.

**Syntax**

```
show users
```

**Parameters**

There are no parameters for this command.

**Default Setting**

This command has no default configuration.

**Command Mode**

User EXEC mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command displays information about the active users.

```
Console# show users

<table>
<thead>
<tr>
<th>Username</th>
<th>Protocol</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bob</td>
<td>Serial</td>
<td></td>
</tr>
<tr>
<td>John</td>
<td>SSH</td>
<td>172.16.0.1</td>
</tr>
<tr>
<td>Robert</td>
<td>HTTP</td>
<td>172.16.0.8</td>
</tr>
<tr>
<td>Betty</td>
<td>Telnet</td>
<td>172.16.1.7</td>
</tr>
</tbody>
</table>
```
**show sessions**

The `show sessions` User EXEC mode command lists open Telnet sessions.

**Syntax**

```
show sessions
```

**Parameters**

There are no parameters for this command.

**Default Setting**

There is no default configuration for this command.

**Command Mode**

User EXEC mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command lists open Telnet sessions.

```
Console> show sessions
```

<table>
<thead>
<tr>
<th>Connection</th>
<th>Host</th>
<th>Address</th>
<th>Port</th>
<th>Byte</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Remote device</td>
<td>172.16.1.1</td>
<td>23</td>
<td>89</td>
</tr>
<tr>
<td>2</td>
<td>172.16.1.2</td>
<td>172.16.1.2</td>
<td>23</td>
<td>8</td>
</tr>
</tbody>
</table>

The following table describes significant fields shown in the example.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection</td>
<td>Connection number.</td>
</tr>
<tr>
<td>Host</td>
<td>Remote host to which the device is connected through a Telnet session.</td>
</tr>
<tr>
<td>Address</td>
<td>IP address of the remote host.</td>
</tr>
<tr>
<td>Port</td>
<td>Telnet TCP port number</td>
</tr>
<tr>
<td>Byte</td>
<td>Number of unread bytes for the user to see on the connection.</td>
</tr>
</tbody>
</table>
show system

The `show system` User EXEC mode command displays system information.

**Syntax**

`show system`

**Parameters**

There are no parameters for this command.

**Default Setting**

This command has no default configuration.

**Command Mode**

User EXEC mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command displays the system information.

```
Console# show system

<table>
<thead>
<tr>
<th>Unit</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>HP 6300</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Unit</th>
<th>Main Power Supply</th>
<th>Redundant Power Supply</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>OPERATION AL</td>
<td>NOT OPERATIONAL</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Fan1</th>
<th>Fan2</th>
<th>Fan3</th>
<th>Fan4</th>
<th>Fan5</th>
</tr>
</thead>
<tbody>
<tr>
<td>OK</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
</tr>
</tbody>
</table>
```
**show version**

The **show version** User EXEC mode command displays system version information.

**Syntax**

```
show version
```

**Parameters**

There are no parameters for this command.

**Default Setting**

This command has no default configuration.

**Command Mode**

User EXEC mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command displays system version information (only for demonstration purposes).

<table>
<thead>
<tr>
<th>SW version</th>
<th>Boot version</th>
<th>HW version</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0.0.0</td>
<td>2.178</td>
<td>1.0.0</td>
</tr>
<tr>
<td>1.0.0.0</td>
<td>2.178</td>
<td>1.0.0</td>
</tr>
</tbody>
</table>
**service cpu-utilization**

The **service cpu-utilization** Global Configuration mode command enables measuring CPU utilization. To return to the default configuration, use the **no** form of this command.

**Syntax**

```
service cpu-utilization
no service cpu-utilization
```

**Parameters**

There are no parameters for this command.

**Default Setting**

Disabled.

**Command Mode**

Global Configuration mode

**Command Usage**

Use the **show cpu utilization** Privileged EXEC command to view information on CPU utilization.

**Example**

The following command enables measuring CPU utilization.

```
Console(config)# service cpu-utilization
```
show cpu utilization

The `show cpu utilization` Privileged EXEC mode command displays information about CPU utilization.

**Syntax**

```
show cpu utilization
```

**Parameters**

There are no parameters for this command.

**Default Setting**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode

**Command Usage**

Use the `service cpu-utilization` Global Configuration mode command to enable measuring CPU utilization.

**Example**

The following command displays CPU utilization information.

```
Console# show cpu utilization

CPU utilization service is on.

CPU utilization
--------------------------------------------------
five seconds: 5%; one minute: 3%; five minutes: 3%
```
tacacs-server host

The **tacacs-server host** Global Configuration mode command specifies a TACACS+ host. To delete the specified name or address, use the **no** form of this command.

**Syntax**

```
tacacs-server host {ip-address | hostname} [single-connection] [port port-number] [timeout timeout] [key key-string] [source source] [priority priority]

no tacacs-server host {ip-address | hostname}
```

**Parameters**

- **ip-address** — IP address of the TACACS+ server.
- **hostname** — Host name of the TACACS+ server. (Range: 1-158 characters)
- **single-connection** — Indicates a single-connection. Rather than have the device open and close a TCP connection to the daemon each time it must communicate, the single-connection option maintains a single open connection between the device and the daemon.
- **port-number** — Specifies a server port number. (Range: 0-65535)
- **timeout** — Specifies the timeout value in seconds. (Range: 1-30)
- **key-string** — Specifies the authentication and encryption key for all TACACS+ communications between the device and the TACACS+ server. This key must match the encryption used on the TACACS+ daemon. To specify an empty string, enter """. (Range: 0-128 characters)
- **source** — Specifies the source IP address to use for the communication. 0.0.0.0 indicates a request to use the IP address of the outgoing IP interface.
- **priority** — Determines the order in which the TACACS+ servers are used, where 0 is the highest priority. (Range: 0-65535)

**Default Setting**

No TACACS+ host is specified.

If no port number is specified, default port number 49 is used.

If no host-specific timeout, key-string or source value is specified, the global value is used.

If no TACACS+ server priority is specified, default priority 0 is used.

**Command Mode**

Global Configuration mode
**Command Usage**

Multiple `tacacs-server host` commands can be used to specify multiple hosts.

**Example**

The following command specifies a TACACS+ host.

```
Console(config)# tacacs-server host 172.16.1.1
```
tacacs-server key

The **tacacs-server key** Global Configuration mode command sets the authentication encryption key used for all TACACS+ communications between the device and the TACACS+ daemon. To disable the key, use the **no** form of this command.

**Syntax**

```
tacacs-server key key-string
no tacacs-server key
```

**Parameters**

- **key-string** — Specifies the authentication and encryption key for all TACACS+ communications between the device and the TACACS+ server. This key must match the encryption used on the TACACS+ daemon. (Range: 0-128 characters)

**Default Setting**

Empty string.

**Command Mode**

Global Configuration mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command sets the authentication encryption key.

```
Console(config)# tacacs-server key hp-s
```
tacacs-server timeout

The tacacs-server timeout Global Configuration mode command sets the interval during which the device waits for a TACACS+ server to reply. To return to the default configuration, use the no form of this command.

Syntax

```
tacacs-server timeout timeout
no tacacs-server timeout
```

Parameters

- **timeout** — Specifies the timeout value in seconds. (Range: 1-30)

Default Setting

5 seconds

Command Mode

Global Configuration mode

Command Usage

There are no user guidelines for this command.

Example

The following command sets the timeout value to 30.

```
Console(config)# tacacs-server timeout 30
```
**tacacs-server source-ip**

The `tacacs-server source-ip` Global Configuration mode command configures the source IP address to be used for communication with TACACS+ servers. To return to the default configuration, use the `no` form of this command.

**Syntax**

```
tacacs-server source-ip source
no tacacs-server source-ip source
```

**Parameters**

- `source` — Specifies the source IP address.

**Default Setting**

The source IP address is the address of the outgoing IP interface.

**Command Mode**

Global Configuration mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command specifies the source IP address.

```
Console(config)# tacacs-server source-ip 172.16.8.1
```
show tacacs

The `show tacacs` Privileged EXEC mode command displays configuration and statistical information about a TACACS+ server.

**Syntax**

```
show tacacs [ip-address]
```

**Parameters**

- `ip-address` — Name or IP address of the TACACS+ server.

**Default Setting**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command displays configuration and statistical information about a TACACS+ server.

```
Console# show tacacs

Device Configuration
--------------------
IP address Status Port Single Connection TimeOut Source IP Priority
---------- ----- --- --------------- ------ -------- ------- -------
          ---- ---- --------------- ----- -------- ------- -------
172.16.1.1 Connected 49 No Global Global 1

Global values
--------------
TimeOut: 3
```

Device Configuration
---------------------
Source IP: 172.16.8.1
**do**

The `do` command executes an EXEC-level command from the Global Configuration mode or any configuration submode.

**Syntax**

`do`

**Parameters**

The EXEC command to be executed.

**Default Setting**

This command has no default configuration.

**Command Mode**

All configuration modes

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command executes an EXEC-level command `show vlan` from the Global Configuration mode.

```
Console(Conf)# do show vlan
```

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Name</th>
<th>Port</th>
<th>Type</th>
<th>Authorization</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>default 2/1-4</td>
<td>1/1-2</td>
<td>other</td>
<td>Required</td>
</tr>
<tr>
<td>10</td>
<td>VLAN0010</td>
<td>1/3-4</td>
<td>dynamic</td>
<td>Required</td>
</tr>
<tr>
<td>11</td>
<td>VLAN0011</td>
<td>1/1-2</td>
<td>static</td>
<td>Required</td>
</tr>
<tr>
<td>20</td>
<td>VLAN0020</td>
<td>1/3-4</td>
<td>static</td>
<td>Required</td>
</tr>
<tr>
<td>21</td>
<td>VLAN0021</td>
<td></td>
<td>static</td>
<td>Required</td>
</tr>
<tr>
<td>30</td>
<td>VLAN0030</td>
<td></td>
<td>static</td>
<td>Required</td>
</tr>
<tr>
<td>31</td>
<td>VLAN0031</td>
<td></td>
<td>static</td>
<td>Required</td>
</tr>
<tr>
<td>91</td>
<td></td>
<td>1/1-2</td>
<td>static</td>
<td>Not required</td>
</tr>
<tr>
<td>3928</td>
<td>GuestVLAN</td>
<td>1/17</td>
<td>static</td>
<td>Guest</td>
</tr>
</tbody>
</table>
enable

The `enable` User EXEC mode command enters the Privileged EXEC mode.

**Syntax**

```
enable [privilege-level]
```

**Parameters**

- `privilege-level` — Privilege level to enter the system. (Range: 1-15)

**Default Setting**

The default privilege level is 15.

**Command Mode**

User EXEC mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command enters the Privileged EXEC mode.

```
Console> enable
   enter password:
   Console#
```
disable

The disable Privileged EXEC mode command returns to the User EXEC mode.

Syntax

disable [privilege-level]

Parameters

■ privilege-level — Privilege level to enter the system. (Range: 1-15)

Default Setting

The default privilege level is 1.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following command returns to Users EXEC mode.

```
Console# disable
Console>
```
**login**

The `login` User EXEC mode command changes a login username.

**Syntax**

```
login
```

**Parameters**

There are no parameters for this command.

**Default Setting**

This command has no default configuration.

**Command Mode**

User EXEC mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command enters Privileged EXEC mode and logs in with username `admin`:

```
Console> login
User Name:admin
Password:*****
Console#
```
**configure**

The `configure` Privileged EXEC mode command enters the Global Configuration mode.

**Syntax**

`configure`

**Parameters**

There are no parameters for this command.

**Default Setting**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command enters the Global Configuration mode.

```
Console# configure
Console(config)#
```
exit (Configuration)

The `exit` command exits any configuration mode to the next highest mode in the CLI mode hierarchy.

**Syntax**

`exit`

**Parameters**

There are no parameters for this command.

**Default Setting**

This command has no default configuration.

**Command Mode**

All configuration modes

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command changes the configuration mode from Interface Configuration mode to Privileged EXEC mode.

```
Console(config)#Console(config-if)# exit
Console(config)# exit
Console#
```
exit

The `exit` Privileged/User EXEC mode command closes an active terminal session by logging off the device.

**Syntax**
exit

**Parameters**
There are no parameters for this command.

**Default Setting**
This command has no default configuration.

**Command Mode**
Privileged and User EXEC modes

**Command Usage**
There are no user guidelines for this command.

**Example**
The following command closes an active terminal session.

```
Console> exit
```
end

The **end** command ends the current configuration session and returns to the Privileged EXEC mode.

**Syntax**

```plaintext
end
```

**Parameters**

There are no parameters for this command.

**Default Setting**

This command has no default configuration.

**Command Mode**

All configuration modes.

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command changes from Global Configuration mode to Privileged EXEC mode.

```
Console(config)# end
Console#
```
help

The `help` command displays a brief description of the help system.

**Syntax**

```
help
```

**Parameters**

There are no parameters for this command.

**Default Setting**

This command has no default configuration.

**Command Mode**

All command modes

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command describes the help system.

```
Console# help
Help may be requested at any point in a command by entering a question mark '?'. If nothing matches the currently entered incomplete command, the help list is empty. This indicates that for a query at this point, there is no command matching the current input. If the request is within a command, enter backspace and erase the entered characters to a point where the request results in a display.

Help is provided when:
1. There is a valid command and a help request is made for entering a parameter or argument (e.g. 'show ?'). All possible parameters or arguments for the entered command are displayed.
2. An abbreviated argument is entered and a help request is made for arguments matching the input (e.g. 'show pr?').
```
**terminal data-dump**

The **terminal data-dump** User EXEC mode command enables dumping all the output of a show command without prompting. To disable dumping, use the **no** form of this command.

**Syntax**

```
terminal data-dump
no terminal data-dump
```

**Parameters**

There are no parameters for this command.

**Default Setting**

Dumping is disabled.

**Command Mode**

User EXEC mode

**Command Usage**

By default, a **More** prompt is displayed when the output contains more lines than can be displayed on the screen. Pressing the **Enter** key displays the next line; pressing the Spacebar displays the next screen of output. The data-dump command enables dumping all output immediately after entering the show command.

This command is relevant only for the current session.

**Example**

The following command dumps all output immediately after entering a show command.

```
Console> terminal data-dump
```
**show history**

The `show history` User EXEC mode command lists the commands entered in the current session.

**Syntax**

```
show history
```

**Parameters**

There are no parameters for this command.

**Default Setting**

This command has no default configuration.

**Command Mode**

User EXEC mode

**Command Usage**

The buffer includes executed and unexecuted commands.

Commands are listed from the first to the most recent command.

The buffer remains unchanged when entering into and returning from configuration modes.

**Example**

The following command displays all the commands entered while in the current Privileged EXEC mode.

```
Console# show history

SW version 3.131 (date 23-Jul-2004 time 17:34:19)
HW version 1.0.0
Console# show clock
15:29:03 Jun 17 2004

Console# show history

show version
show clock
show history
3 commands were logged (buffer size is 10)
```
show privilege

The show privilege Privileged/User EXEC mode command displays the current privilege level.

Syntax

show privilege

Parameters

There are no parameters for this command.

Default Setting

This command has no default configuration.

Command Mode

Privileged and User EXEC modes

Command Usage

There are no user guidelines for this command.

Example

The following command displays the current privilege level for the Privileged EXEC mode.

```
Console# show privilege
Current privilege level is 15
```
VLAN Commands

`vlan database`

The `vlan database` Global Configuration mode command enters the VLAN Configuration mode.

**Syntax**

`vlan database`

**Parameters**

There are no parameters for this command.

**Default Setting**

Two VLANs are assigned in the VLAN database:

- VLAN 1
- VLAN 2

**Command Mode**

Global Configuration mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command enters the VLAN database mode.

```
Console(config)# vlan database
console(config-vlan)#
```
**vlan**

Use the **vlan** VLAN Configuration mode command to create a VLAN. To delete a VLAN, use the **no** form of this command.

**Syntax**

```
vlan vlan-range
no vlan vlan-range
```

**Parameters**

- **vlan-range** — Specifies a list of VLAN IDs to be added. Separate nonconsecutive VLAN IDs with a comma and no spaces; a hyphen designates a range of IDs.

**Default Setting**

This command has no default configuration.

**Command Mode**

VLAN Configuration mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command VLAN number 1972 is created.

```
Console(config)# vlan database
console(config-vlan)# vlan 1972
```
**interface vlan**

The *interface vlan* Global Configuration mode command enters the Interface Configuration (VLAN) mode.

**Syntax**

```
interface vlan vlan-id
```

**Parameters**

- *vlan-id* — Specifies an existing VLAN ID.

**Default Setting**

Two interfaces are configured and set to DHCP:

- one on VLAN 1
- one on VLAN 2

**Command Mode**

Global Configuration mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command configures VLAN 1 with IP address 131.108.1.27 and subnet mask 255.255.255.0.

```console
Console(config)# interface vlan 1
Console(config-if)# ip address 131.108.1.27 255.255.255.0
```
interface range vlan

The interface range vlan Global Configuration mode command enables simultaneously configuring multiple of VLANs.

Syntax

interface range vlan {vlan-range | all}

Parameters

■ vlan-range — Specifies a list of VLAN IDs to be added. Separate nonconsecutive VLAN IDs with a comma and no spaces; a hyphen designates a range of IDs.

■ all — All existing static VLANs.

Default Setting

This command has no default configuration.

Command Mode

Global Configuration mode

Command Usage

Commands under the interface range context are executed independently on each interface in the range. If the command returns an error on one of the interfaces, an error message is displayed and execution of the command continues on the other interfaces.

Example

The following command groups VLANs 221 to 228 and 889 to receive the same command.

```
Console(config)# interface range vlan 221-228,889
Console(config-if)#
```
name

The **name** Interface Configuration mode command adds a name to a VLAN. To remove the VLAN name, use the **no** form of this command.

**Syntax**

```plaintext
name string
no name
```

**Parameters**

- `string` — Unique name to be associated with this VLAN. (Range: 1-32 characters)

**Default Setting**

No name is defined.

**Command Mode**

Interface Configuration (VLAN) mode. Cannot be configured for a range of interfaces (range context).

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command gives VLAN number 19 the name **Marketing**.

```plaintext
Console(config)# interface vlan 19
Console(config-if)# name Marketing
```
**switchport mode**

The **switchport mode** Interface Configuration mode command configures the VLAN membership mode of a port. To return to the default configuration, use the **no** form of this command.

**Syntax**

```
switchport mode {access | trunk | general}
no switchport mode
```

**Parameters**

- **access** — Indicates an untagged layer 2 VLAN port.
- **trunk** — Indicates a trunking layer 2 VLAN port.
- **general** — Indicates a full 802-1q supported VLAN port.

**Default Setting**

All ports are in access mode. All ports do not all belong to the default VLAN. By default, odd ports 1-41, 42, 45, and 46 are all in VLAN 1. The remaining ports are in VLAN 2.

**Command Mode**

Interface Configuration (Ethernet, port-channel) mode

**Command Usage**

There are no user guidelines.

**Example**

The following command configures Ethernet port 1/e16 as an untagged layer 2 VLAN port.

```
Console(config)# interface ethernet 1/e16
Console(config-if)# switchport mode access
```
switchport access vlan

The switchport access vlan Interface Configuration mode command configures the VLAN ID when the interface is in access mode. To return to the default configuration, use the no form of this command.

Syntax

switchport access vlan {vlan-id | dynamic}
no switchport access vlan

Parameters

- vlan-id — Specifies the ID of the VLAN to which the port is configured.
- dynamic — Indicates that the port is assigned to a VLAN based on the source MAC address of the host connected to the port.

Default Setting

Odd ports 1-41, 42, 45, and 46 are all in VLAN 1. The remaining ports are in VLAN 2.

Command Mode

Interface configuration (Ethernet, port-channel) mode

Command Usage

The command automatically removes the port from the previous VLAN and adds it to the new VLAN.

Example

The following command configures Ethernet port 1/e16 in access mode to be member of VLAN 23.

```
Console(config)# interface ethernet 1/e16
Console(config-if)# switchport access vlan 23
```
switchport trunk allowed vlan

The `switchport trunk allowed vlan` Interface Configuration mode command adds or removes VLANs to or from a trunk port.

**Syntax**

```
switchport trunk allowed vlan {add vlan-list | remove vlan-list}
```

**Parameters**

- `add vlan-list` — List of VLAN IDs to be added. Separate nonconsecutive VLAN IDs with a comma and no spaces. A hyphen designates a range of IDs.
- `remove vlan-list` — List of VLAN IDs to be removed. Separate nonconsecutive VLAN IDs with a comma and no spaces. A hyphen designates a range of IDs.

**Default Setting**

This command has no default configuration.

**Command Mode**

Interface Configuration (Ethernet, port-channel) mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command adds VLANs 1, 2, 5 to 6 to the allowed list of Ethernet port 1/e16.

```
Console(config)# interface ethernet 1/e16
Console(config-if)# switchport trunk allowed vlan add 1-2,5-6
```
**switchport trunk native vlan**

The `switchport trunk native vlan` Interface Configuration mode command defines the native VLAN when the interface is in trunk mode. To return to the default configuration, use the `no` form of this command.

**Syntax**

```
switchport trunk native vlan vlan-id
no switchport trunk native vlan
```

**Parameters**

- `vlan-id`— Specifies the ID of the native VLAN.

**Default Setting**

VID=1.

**Command Mode**

Interface Configuration (Ethernet, port-channel) mode

**Command Usage**

The command adds the port as a member in the VLAN. If the port is already a member in the VLAN (not as a native), it should be first removed from the VLAN.

**Example**

The following command configures VLAN number 123 as the native VLAN when Ethernet port 1/e16 is in trunk mode.

```
Console(config)# interface ethernet 1/e16
Console(config-if)# switchport trunk native vlan 123
```
VLAN Commands

**switchport general allowed vlan**

The `switchport general allowed vlan` Interface Configuration mode command adds or removes VLANs from a general port.

**Syntax**

```
switchport general allowed vlan add vlan-list [tagged | untagged]
switchport general allowed vlan remove vlan-list
```

**Parameters**

- **add vlan-list** — Specifies the list of VLAN IDs to be added. Separate nonconsecutive VLAN IDs with a comma and no spaces. A hyphen designates a range of IDs.
- **remove vlan-list** — Specifies the list of VLAN IDs to be removed. Separate nonconsecutive VLAN IDs with a comma and no spaces. A hyphen designates a range of IDs.
- **tagged** — Indicates that the port transmits tagged packets for the VLANs.
- **untagged** — Indicates that the port transmits untagged packets for the VLANs.

**Default Setting**

If the port is added to a VLAN without specifying tagged or untagged, the default setting is tagged.

**Command Mode**

Interface Configuration (Ethernet, port-channel) mode

**Command Usage**

This command enables changing the egress rule (e.g., from tagged to untagged) without first removing the VLAN from the list.

**Example**

The following commands add VLANs 2, 5, and 6 to the allowed list of Ethernet port 1/e16.

```
Console(config)# interface ethernet 1/e16
Console(config-if)# switchport general allowed vlan add 2,5-6 tagged
```
switchport general pvid

The `switchport general pvid` Interface Configuration mode command configures the PVID when the interface is in general mode. To return to the default configuration, use the **no** form of this command.

**Syntax**

`switchport general pvid vlan-id`

`no switchport general pvid`

**Parameters**

- `vlan-id` — Specifies the PVID (Port VLAN ID).

**Default Setting**

If the default VLAN is enabled, PVID = 1. Otherwise, PVID=4095.

**Command Mode**

Interface Configuration (Ethernet, port-channel) mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following commands configure the PVID for Ethernet port 1/e16, when the interface is in general mode.

```
Console(config)# interface ethernet 1/e16
Console(config-if)# switchport general pvid 234
```
switchport general ingress-filtering disable

The switchport general ingress-filtering disable Interface Configuration mode command disables port ingress filtering. Ingress filtering discards frames to VLAN where port does not belong. To return to the default configuration, use the no form of this command.

Syntax

switchport general ingress-filtering disable
no switchport general ingress-filtering disable

Parameters

There are no parameters for this command.

Default Setting

Ingress filtering is enabled.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

Command Usage

There are no user guidelines for this command.

Example

The following commands disable port ingress filtering on Ethernet port 1/e16.

```
Console(config)# interface ethernet 1/e16
Console(config-if)# switchport general ingress-filtering disable
```
switchport general acceptable-frame-type tagged-only

The switchport general acceptable-frame-type tagged-only Interface Configuration mode command discards untagged frames at ingress. To return to the default configuration, use the no form of this command.

Syntax
switchport general acceptable-frame-type tagged-only
no switchport general acceptable-frame-type tagged-only

Parameters
There are no parameters for this command.

Default Setting
All frame types are accepted at ingress.

Command Mode
Interface Configuration (Ethernet, port-channel) mode

Command Usage
There are no user guidelines for this command.

Example
The following commands configure Ethernet port 1/e16 to discard untagged frames at ingress.

```
Console(config)# interface ethernet 1/e16
Console(config-if)# switchport general acceptable-frame-type tagged-only
```
switchport forbidden vlan

The switchport forbidden vlan Interface Configuration mode command forbids adding specific VLANs to a port. To return to the default configuration, use the remove parameter for this command.

**Syntax**

switchport forbidden vlan {add vlan-list | remove vlan-list}

**Parameters**

- **add vlan-list** — Specifies the list of VLAN IDs to be added. Separate nonconsecutive VLAN IDs with a comma and no spaces. A hyphen designates a range of IDs.
- **remove vlan-list** — Specifies the list of VLAN IDs to be removed. Separate nonconsecutive VLAN IDs with a comma and no spaces. A hyphen designates a range of IDs.

**Default Setting**

All VLANs are allowed.

**Command Mode**

Interface Configuration (Ethernet, port-channel) mode

**Command Usage**

This command can be used to prevent GVRP from automatically making the specified VLANs active on the selected ports.

**Example**

The following command forbids adding VLAN IDs 234 to 256 to Ethernet port 1/e16.

```
Console(config)# interface ethernet 1/e16
Console(config-if)# switchport forbidden vlan add 234-256
```
**ip internal-usage-vlan**

The **ip internal-usage-vlan** Interface Configuration mode command reserves a VLAN as the internal usage VLAN of an interface. To return to the default configuration, use the **no** form of this command.

**Syntax**

```
ip internal-usage-vlan vlan-id
no ip internal-usage-vlan
```

**Parameters**

- **vlan-id** — Specifies the ID of the internal usage VLAN.

**Default Setting**

The software reserves a VLAN as the internal usage VLAN of an interface.

**Command Mode**

Interface Configuration (Ethernet, port-channel) mode

**Command Usage**

- An internal usage VLAN is required when an IP interface is configured on an Ethernet port or port-channel.
- This command enables the user to configure the internal usage VLAN of a port. If an internal usage VLAN is not configured and the user wants to configure an IP interface, an unused VLAN is selected by the software.
- If the software selected a VLAN for internal use and the user wants to use that VLAN as a static or dynamic VLAN, the user should do one of the following:
  - Remove the IP interface.
  - Use this command to explicitly configure a different VLAN as the internal usage VLAN.
  - Create the VLAN and recreate the IP interface.

**Example**

The following command reserves an unused VLAN 1236 as the internal usage VLAN of ethernet port 1/e8.

```
Console(config)# interface ethernet 1/e8
Console(config-if)# ip internal-usage-vlan 1236
```
show vlan

The show vlan Privileged EXEC mode command displays VLAN information.

Syntax

show vlan [id vlan-id] name vlan-name]

Parameters

- vlan-id — specifies a VLAN ID
- vlan-name — Specifies a VLAN name string. (Range: 1-32 characters)

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following command displays all VLAN information.

```
Console# show vlan

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Name</th>
<th>Ports</th>
<th>Type</th>
<th>Authorization</th>
</tr>
</thead>
<tbody>
<tr>
<td>----</td>
<td>-------</td>
<td>-----------</td>
<td>-----</td>
<td>--------------</td>
</tr>
<tr>
<td>1</td>
<td>default</td>
<td>1/e1-e2,</td>
<td>other</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2/e1-e4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>VLAN0010</td>
<td>1/e3-e4</td>
<td>dynamic</td>
<td>Required</td>
</tr>
<tr>
<td>11</td>
<td>VLAN0011</td>
<td>1/e1-e2</td>
<td>static</td>
<td>Required</td>
</tr>
<tr>
<td>20</td>
<td>VLAN0020</td>
<td>1/e3-e4</td>
<td>static</td>
<td>Required</td>
</tr>
<tr>
<td>21</td>
<td>VLAN0021</td>
<td>1/e3-e4</td>
<td>static</td>
<td>Required</td>
</tr>
<tr>
<td>30</td>
<td>VLAN0030</td>
<td>static</td>
<td></td>
<td>Required</td>
</tr>
<tr>
<td>31</td>
<td>VLAN0031</td>
<td>static</td>
<td></td>
<td>Required</td>
</tr>
<tr>
<td>91</td>
<td>VLAN0011</td>
<td>1/e1-e2</td>
<td>static</td>
<td>Not Required</td>
</tr>
<tr>
<td>3978</td>
<td>Guest VLAN</td>
<td>1/e17</td>
<td>guest</td>
<td></td>
</tr>
</tbody>
</table>
```
**show vlan internal usage**

The `show vlan internal usage` Privileged EXEC mode command displays a list of VLANs used internally by the device.

**Syntax**

```
show vlan internal usage
```

**Parameters**

There are no parameters for this command.

**Default Setting**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command displays VLANs used internally by the device.

```
Console# show vlan internal usage

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Usage</th>
<th>IP Address</th>
<th>Reserved</th>
</tr>
</thead>
<tbody>
<tr>
<td>1007</td>
<td>Eth 1/e21</td>
<td>Active</td>
<td>No</td>
</tr>
<tr>
<td>1008</td>
<td>Eth 1/e22</td>
<td>Inactive</td>
<td>Yes</td>
</tr>
<tr>
<td>1009</td>
<td>Eth 1/e23</td>
<td>Active</td>
<td>Yes</td>
</tr>
</tbody>
</table>
```
**show interfaces switchport**

The `show interfaces switchport` Privileged EXEC mode command displays the switchport configuration.

**Syntax**

`show interfaces switchport {ethernet interface | port-channel port-channel-number}`

**Parameters**

- `interface` — A valid Ethernet port number.
- `port-channel-number` — A valid port-channel number.

**Default Setting**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command displays the switchport configuration for Ethernet port 1/e1.

```
Console# show interface switchport ethernet 1/e1

Port 1/e1:
VLAN Membership mode: General

Operating parameters:
PVID: 1 (default)
Ingress Filtering: Enabled
Acceptable Frame Type: All
GVRP status: Enabled
Protected: Enabled, Uplink is 1/e9.

Port 1/e1 is member in:
<table>
<thead>
<tr>
<th>VLAN</th>
<th>Name</th>
<th>Egress Rule</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>----</td>
<td>--------------</td>
<td>-------------</td>
<td>--------</td>
</tr>
<tr>
<td>1</td>
<td>default</td>
<td>untagged</td>
<td>System</td>
</tr>
<tr>
<td>8</td>
<td>VLAN008</td>
<td>tagged</td>
<td>Dynamic</td>
</tr>
<tr>
<td>11</td>
<td>VLAN011</td>
<td>tagged</td>
<td>Static</td>
</tr>
<tr>
<td>19</td>
<td>IPv6 VLAN</td>
<td>untagged</td>
<td>Static</td>
</tr>
<tr>
<td>72</td>
<td>VLAN0072</td>
<td>untagged</td>
<td>Static</td>
</tr>
</tbody>
</table>
```
Static configuration:
PVID: 1 (default)
Ingress Filtering: Enabled
Acceptable Frame Type: All

Port 1/e1 is statically configured to:

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Name</th>
<th>Egress Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>default</td>
<td>untagged</td>
</tr>
<tr>
<td>11</td>
<td>VLAN011</td>
<td>tagged</td>
</tr>
<tr>
<td>19</td>
<td>IPv6 VLAN</td>
<td>untagged</td>
</tr>
<tr>
<td>72</td>
<td>VLAN0072</td>
<td>untagged</td>
</tr>
</tbody>
</table>

Forbidden VLANS:

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>73</td>
<td>out</td>
</tr>
</tbody>
</table>

Console# `show interface switchport ethernet 1/e2`

Port 1/e2:
VLAN Membership mode: General

Operating parameters:
PVID: 4095 (discard vlan)
Ingress Filtering: Enabled
Acceptable Frame Type: All

Port 1/e1 is member in:

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Name</th>
<th>Egress Rule</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>91</td>
<td>IP Telephony</td>
<td>tagged</td>
<td>Static</td>
</tr>
</tbody>
</table>

Static configuration:
PVID: 8
Ingress Filtering: Disabled
Acceptable Frame Type: All
**VLAN Commands**

Port 1/e2 is statically configured to:

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Name</th>
<th>Egress rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>VLAN0072</td>
<td>untagged</td>
</tr>
<tr>
<td>91</td>
<td>IP Telephony</td>
<td>tagged</td>
</tr>
</tbody>
</table>

Forbidden VLANS:

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>73</td>
<td>out</td>
</tr>
</tbody>
</table>

Port 2/e19

Static configuration:
- PVID: 2922
- Ingress Filtering: Enabled
- Acceptable Frame Type: Untagged
- GVRP status: Disabled
Web Server Commands

ip http server

The `ip http server` Global Configuration mode command enables configuring the device from a browser. To disable this function, use the `no` form of this command.

**Syntax**

```
ip http server
no ip http server
```

**Parameters**

There are no parameters for this command.

**Default Setting**

HTTP server is enabled.

**Command Mode**

Global Configuration

**Command Usage**

Only a user with access level 15 can use the Web server.

**Example**

The following command enables configuring the device from a browser.

```
Console(config)# Console(config)# ip http server
```
**ip http port**

The `ip http port` Global Configuration mode command specifies the TCP port to be used by the Web browser interface. To return to the default configuration, use the `no` form of this command.

**Syntax**

```
ip http port port-number
no ip http port
```

**Parameters**

- `port-number` — Port number for use by the HTTP server. (Range: 0-65535)

**Default Setting**

The default port number is 80.

**Command Mode**

Global Configuration

**Command Usage**

Specifying 0 as the port number effectively disables HTTP access to the device.

**Example**

The following command configures the http port number to 100.

```
Console(config)# ip http port 100
```
**ip https server**

The **ip https server** Global Configuration mode command enables configuring the device from a secured browser. To return to the default configuration, use the **no** form of this command.

**Syntax**

**ip https server**
**no ip https server**

**Parameters**

There are no parameters for this command.

**Default Setting**

HTTPS server disabled.

**Command Mode**

Global Configuration mode

**Command Usage**

Use the **crypto certificate generate** Global Configuration mode command to generate an HTTPS certificate.

**Example**

The following command enables configuring the device from a secured browser.

```console
Console(config)# ip https server
```
ip https port

The **ip https port** Global Configuration mode command specifies the TCP port used by the server to configure the device through the Web browser. To return to the default configuration, use the `no` form of this command.

**Syntax**

```
ip https port port-number
no ip https port
```

**Parameters**

- `port-number` — Port number to be used by the HTTP server. (Range: 0-65535)

**Default Setting**

The default port number is 443.

**Command Mode**

Global Configuration mode

**Command Usage**

Specifying 0 as the port number effectively disables HTTPS access to the device.

**Example**

The following command configures the https port number to 100.

```
Console(config)# Console(config)# ip https port 100
```
crypto certificate generate

The crypto certificate generate Global Configuration mode command generates a self-signed HTTPS certificate.

Syntax

crypto certificate [number] generate [key-generate [length]] [cn common-name] [ou organization-unit] [or organization] [loc location] [st state] [cu country] [duration days]

Parameters

- number — Specifies the certificate number. (Range: 1-2)
- key-generate — Regenerate the SSL RSA key.
- length — Specifies the SSL RSA key length. (Range: 512-2048)
- common-name — Specifies the fully qualified URL or IP address of the device. (Range: 1-64)
- organization — Specifies the organization name. (Range: 1-64)
- organization-unit — Specifies the organization-unit or department name. (Range: 1-64)
- location — Specifies the location or city name. (Range: 1-64)
- state — Specifies the state or province name. (Range: 1-64)
- country — Specifies the country name. (Range: 2-2)
- days — Specifies number of days certification is valid. (Range: 30-3650)

Default Setting

The Certificate and SSL’s RSA key pairs do not exist.

If no certificate number is specified, the default certificate number is 1.

If no RSA key length is specified, the default length is 1024.

If no URL or IP address is specified, the default common name is the lowest IP address of the device at the time that the certificate is generated.

If the number of days is not specified, the default period of time that the certification is valid is 365 days.

Command Mode

Global Configuration mode

Command Usage

The command is not saved in the device configuration; however, the certificate and keys generated by this command are saved in the private configuration (which is never displayed to the user or backed up to another device).

Use this command to generate a self-signed certificate for the device.

If the RSA keys do not exist, parameter key-generate must be used.
Example

The following command regenerates an HTTPS certificate.

```
Console(config)# crypto certificate 1 generate key-generate
```
**crypto certificate request**

The **crypto certificate request** Privileged EXEC mode command generates and displays certificate requests for HTTPS.

**Syntax**

```plaintext
crypto certificate number request [cn common-name] [ou organization-unit] [or organization] [loc location] [st state] [cu country]
```

**Parameters**

- **number** — Specifies the certificate number. (Range: 1-2)
- **common-name** — Specifies the fully qualified URL or IP address of the device. (Range: 1-64)
- **organization-unit** — Specifies the organization-unit or department name. (Range: 1-64)
- **organization** — Specifies the organization name. (Range: 1-64)
- **location** — Specifies the location or city name. (Range: 1-64)
- **state** — Specifies the state or province name. (Range: 1-64)
- **country** — Specifies the country name. (Range: 1-2)

**Default Setting**

There is no default configuration for this command.

**Command Mode**

Privileged EXEC mode

**Command Usage**

Use this command to export a certificate request to a Certification Authority. The certificate request is generated in Base64-encoded X.509 format.

Before generating a certificate request you must first generate a self-signed certificate using the **crypto certificate generate** Global Configuration mode command. Be aware that you have to reenter the certificate fields.

After receiving the certificate from the Certification Authority, use the **crypto certificate import** Global Configuration mode command to import the certificate into the device. This certificate replaces the self-signed certificate.
**Example**

The following command generates and displays a certificate request for HTTPS.

```bash
Console# crypto certificate 1 request

-----BEGIN CERTIFICATE REQUEST-----
MIwTCCSoCAQAwYjELMAkGA1UEBhMCUFAXczAJBgNVBAgTAKNDMQswCQYDVQQL
ErRDEMMAoGA1UEChMDZGw0wCgYDVQQLEwNkbGQxCzAJBgNVBAMTAmxkMRAw
HdML083110fn/F0MV/Kib6Sz5p+3nUUnenbHbHp/gVPMFM+1nbqTDezb2ymCu6K
aKVebVLF9F2LmM7VpJDBb9bb4jnxkvwW/wzDLvW2rse5NyPmH1lQV1+8Ubx3GyCm
/oW93BSOFxwvEsE5S8kI+sPYPy+/8wwmoNlDwiDAQABoB8wHQACYKoZlhcvNQnkH
MRDjEyMwigICCAgIICAICAgIMAOGCSqGSIb3DQEBBAUA4GBAAb8Uglkx7rB05m+2
m5ZPlh1w8ARSPXwhVdJxvFbnmwcacgP8piRv6LkxryGF2bVU3jKEipczA
g+uNpyTkDl3ZVU72piz/8a8TF0n3
-----END CERTIFICATE REQUEST-----
CN= router.gm.com
O= General Motors
C= US
```
**crypto certificate import**

The **crypto certificate import** Global Configuration mode command imports a certificate signed by the Certification Authority for HTTPS.

**Syntax**

crypto certificate number import

**Parameters**

- **number** — Specifies the certificate number. (Range: 1-2)

**Default Setting**

This command has no default configuration.

**Command Mode**

Global Configuration mode

**Command Usage**

Use this command to enter an external certificate (signed by Certification Authority) to the device. To end the session, enter an empty line.

The imported certificate must be based on a certificate request created by the **crypto certificate request** Privileged EXEC mode command.

If the public key found in the certificate does not match the device’s SSL RSA key, the command fails.

This command is not saved in the device configuration; however, the certificate imported by this command is saved in the private configuration (which is never displayed to the user or backed up to another device).
Example

The following command imports a certificate signed by Certification Authority for HTTPS.

```bash
Console(config)# crypto certificate 1 import

-----BEGIN CERTIFICATE-----
<CERTIFICATE CONTENT>
Certificate imported successfully.
Issued to: router.gm.com
Issued by: www.verisign.com
Subject: CN= router.gm.com, 0= General Motors, C= US
Finger print: DC789788 DC88A988 127897BC BB789788
-----END CERTIFICATE-----
```
**ip https certificate**

The *ip https certificate* Global Configuration mode command configures the active certificate for HTTPS. To return to the default configuration, use the *no* form of this command.

**Syntax**

```
ip https certificate number
no ip https certificate
```

**Parameters**

- `number` — Specifies the certificate number. (Range: 1-2)

**Default Setting**

Certificate number 1.

**Command Mode**

Global Configuration mode

**Command Usage**

The *crypto certificate generate* command should be used to generate HTTPS certificates.

**Example**

The following command configures the active certificate for HTTPS.

```
Console(config)#Console(config)# ip https certificate 1
```
show crypto certificate mycertificate

The show crypto certificate mycertificate Privileged EXEC mode command displays the SSH certificates of the device.

Syntax

show crypto certificate mycertificate [number]

Parameters

- number — Specifies the certificate number. (Range: 1-2)

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following command displays the certificate.

```
Console# show crypto certificate mycertificate 1

-----BEGIN CERTIFICATE-----
dHmUgUm9vdCBDZXJ0aWZpZXlwaXQgY29udGV4dCBwYXluZ3MgZm9ydCBhbmQg
nnH/xQSQA2fkkRBoUIZtHb7n8VPSQm1xyJ1t1a1Ga8cHfMqgeOZm9fhoHSWr
vf1FpDOMW07GwaQAo4IBojCCCAAZ4wEwYJKwYBBAGCNxQCBAYeBABDAEw
CwR0PBAOQDAgFiGBA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYEFAf4MT9BRD4
ZvKBAGL9Gpp+6MiIIBNgYVR0IBII8LCTCCASKwdKggc+ggcyGcIsZGFwOi8v
LOVByb3hISJTwU29mdHdcmUiMjBSb290JTwQ2VydGlmaWwyLENOPXICnZl
-----END CERTIFICATE-----

Issued by: www.verisign.com
Subject: CN= router.gm.com, O= General Motors, C= US
Finger print: DC789788 DC88A988 1278978C BB789788
```
show ip http

The show ip http Privileged EXEC mode command displays the HTTP server configuration.

**Syntax**

```
show ip http
```

**Parameters**

There are no parameters for this command.

**Default Setting**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command displays the HTTP server configuration.

```
Console# show ip http
HTTP server enabled. Port: 80
```
show ip https

The `show ip https` Privileged EXEC mode command displays the HTTPS server configuration.

**Syntax**

`show ip https`

**Parameters**

There are no parameters for this command.

**Default Setting**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode

**Command Usage**

There are no user guidelines for this command.

**Example**

The following command displays the HTTP server configuration.

```
Console# show ip https

HTTPS server enabled. Port: 443

Certificate 1 is active
 Issued by: www.verisign.com
 Valid from: 8/9/2004 to 8/9/2005
 Subject: CN= router.gm.com, O= General Motors, C= US
 Finger print: DC789788 DC88A988 127897BC BB789788

Certificate 2 is inactive
 Issued by: self-signed
 Subject: CN= router.gm.com, O= General Motors, C= US
 Finger print: 1873B936 88DC3411 BC8932EF 782134BA
```
A
AAA commands 3–1 to 3–12
    defined 1–7
abbreviations 1–3
abort MST 22–25
Access Control List (ACL) configuration 1–5
access lists 4–12
access mode
    normal 1–1
    privileged 1–1
accessing
    Command Line Interface 1–1
    switch through console port 1–1
ACL commands 4–1 to 4–12
    defined 1–7
address table commands 5–1 to 5–21
    defined 1–7
alarm 20–9
arguments 1–3
arp
    clear 11–7
    show 11–8
    timeout 11–6
arrows 1–6
authentication
    AAA 3–1
    aaa enable 3–3
    enable 3–6
    ip http 3–7
    ip https 3–8
    login 3–5
    show methods 3–9
B
back pressure 8–10
boot system 7–5
bridge commands 5–1 to 5–9, 5–14 to 5–19
C
class 18–8
class map 18–3
clear counters 8–11
clear host 11–13
clearing
    logging 24–6
clock
    set 6–1
    show 6–16
    source 6–2
    summer time 6–4
    timezone 6–3
clock commands 6–1 to 6–18
    defined 1–7
command line interface See CLI
command line processing 1–6
commands
    abbreviation 1–3
    completion 1–3
    entering 1–3
    groups 1–7
    help 1–3
    history 1–4
    keystroke 1–6
    modes 1–4
    negating 1–4
    showing 1–3
configuration 7–6, 7–7
    gvrp 9–7
Configuration class 1–4
configuration commands 1–4, 1–5, 7–1 to 7–8
    defined 1–7
configuration, storing 1–5
configure, Privileged EXEC mode 27–5
connecting to switch 1–1
connections, Telnet 1–1
console connection 1–1
copper ports 15–2, 15–3
copy 7–1
CoS 18–28
counters 8–11, 8–17
cpu utilization 25–15, 25–16
CRC align errors 20–2
crypto certificate generate 29–5
current configuration 7–6

database, VLAN 28–1
delete 7–4
deny 14–4
deny (IP) 4–5
deny (MAC) 4–9
description 8–4
dhcp 11–2, 11–14
DHCP configuration 1–5
disable
  Privileged EXEC mode 27–3
displaying spanning tree information 22–27
do 27–1
domain lookup 11–9
dot1x commands 2–1 to 2–23
duplex 8–6

enable
  GVRP 9–1, 9–2
  Privileged EXEC mode 27–2
enable password 3–10, 3–11
end 27–8
entering
  commands 1–3
  multiple commands 1–3
ethernet configuration commands 8–1 to 8–23
  defined 1–7
Exec class 1–4
Exec commands 1–4
exit 27–6, 27–7
exit MST 22–24

fiber ports 15–4
flowcontrol 8–8

garp timer 9–3
global configuration 1–5
groups
  commands 1–7
GVRP commands 9–1 to 9–9
  defined 1–7

help 1–3, 27–9
history 1–4, 13–5, 27–11
history size 13–6
host
  clear 11–13
  IP
    host 11–12
    show 11–15
hostname 25–10

IGMP snooping commands 10–1 to 10–9
  defined 1–7
image file commands 7–1 to 7–8
  defined 1–7
instance MST 22–20
interface configuration 1–5
interface value 8–12
interfaces
  active 8–12
  advertise 8–13
  configuration 8–14
  counters 8–17
  description 8–16
  status 8–15
IP
  domain lookup 11–9
  HTTP port 29–2
  HTTPS port 29–4
  HTTPS server 29–3
IP address, switch 1–1
IP addressing commands 11–1 to 11–15
  defined 1–7
jabbers 20–2

key string 23–8
keystroke commands 1–6
keywords 1–3
  partial lookup 1–4
keywords table 25–6

LACP commands 12–1 to 12–6
  defined 1–7
line commands 13–1 to 13–9
  defined 1–7
line configuration 1–5
listing current valid commands 1–4
login authentication 3–5
login User EXEC mode 27–4
looking up partial keywords 1–4
| M | mac access list 4–7  
management ACL commands 14–1 to 14–7  
  defined 1–7  
  match 18–6  
  mdix 8–9  
MSTP configuration 1–5  
multiple commands 1–3 |
|---|---|
| N | name 28–5  
  name MST 22–21  
negating commands 1–4  
negotiation 8–7  
normal access mode 1–1 |
| O | octets 20–2  
opening  
  Telnet session 1–1  
opening, Telnet session 1–2 |
| P | packets 20–2  
parameters 1–3  
password 3–10  
  enable 3–10, 3–11  
  permit 14–3  
  permit (IP) 4–2  
  permit (MAC) 4–8  
PHY diagnostic commands  
  defined 1–7  
PHY diagnostics commands 15–1 to 15–4  
ping 25–1  
police 18–12  
policy map 18–7  
port channel commands 16–1 to 16–4  
  defined 1–7  
port monitor commands 17–1 to 17–3  
  defined 1–7  
port security 5–10, 5–20  
  max 5–12  
  mode 5–11  
  routed secure address 5–13  
ports table 25–6  
privileged access mode 1–1  
processing 1–6 |
| Q | QoS commands 18–1 to 18–29  
  defined 1–7 |
| R | RADIUS commands 19–1 to 19–8  
  defined 1–8  
reload 25–9  
resume 25–8  
revision MST 22–22  
RMON commands 20–1 to 20–17  
  defined 1–8  
router configuration 1–5  
running configuration 7–6 |
| S | security  
  port 5–10  
  port max 5–12  
  port mode 5–11  
  port routed secure-address 5–13  
  show ports 5–20  
  show ports addresses 5–21  
service acl 4–11  
service cpu utilization 25–15  
service policy 18–13  
sessions, show 25–13  
set 18–11  
  interface value 8–12  
show  
  access lists 4–12  
  arp 11–8  
  authentication methods 3–9  
  bootvar 7–8  
  class map 18–5  
  clock 6–16  
  copper ports 15–2, 15–3  
  cpu utilization 25–16  
  fiber ports 15–4  
  gvrp configuration 9–7  
  gvrp statistics 9–8  
  history 27–11  
  hosts 11–15  
  interfaces advertise 8–13  
  interfaces configuration 8–14  
  interfaces counters 8–17  
  interfaces description 8–16  
  interfaces port channel 16–4  
  interfaces status 8–15  
  IP HTTP 29–13  
  IP HTTPS 29–14  
  ip igmp snooping 10–7, 10–8, 10–9  
  IP interface 11–4  
  IP SSH 23–10 |